数学名著译丛

博大精深的素数

〔加拿大〕P．里本伯姆　著
孙淑玲　冯克勤　译



数学名著译丛

博大精深的素数

〔加拿大〕P. 里本伯姆　著

孙淑玲　冯克勤　译

科学出版社

北　京

图字：01-2006-2858 号

内 容 简 介

本书介绍了从欧几里得、费马、欧拉、高斯以来2000多年中素数研究的重要成果、问题、思想和方法，包括素数有多少、如何识别素数、是否有定义素数的函数等一系列具有重要理论意义和应用背景的问题，并介绍了相关问题至2003年的最新记录.

本书内容全面、新颖，可供大学数学系高年级学生、研究生、教师以及从事数学、信息科学等工作的科研人员阅读参考.

图书在版编目(CIP)数据

博大精深的素数/(加拿大)P. 里本伯姆著；孙淑玲，冯克勤 译. —北京：科学出版社，2007
(数学名著译丛)
ISBN 978-7-03-017370-6

I. 博… II. ①P… ②孙… ③冯… III. 素数-普及读物 IV. O156.2-49

中国版本图书馆 CIP 数据核字(2006)第 058449 号

责任编辑：吕 虹 张 扬 张启男 杨 然/责任校对：张小霞
责任印制：安春生/封面设计：王 浩

科 学 出 版 社 出版
北京东黄城根北街 16 号
邮政编码：100717
http://www.sciencep.com

新 蕾 印 刷 厂 印刷

科学出版社编务公司排版制作
科学出版社发行 各地新华书店经销

*

2007年1月第 一 版 开本：(850×1168) 1/32
2007年1月第一次印刷 印张：11 1/4
印数：1—3 000 字数：288 000

定价：38.00 元

(如有印装质量问题，我社负责调换〈环伟〉)

前　言

《吉尼斯记录大全》一书已家喻户晓. 人们在喝具有吉尼斯商标烈性啤酒时进行友好的争辩，此书成为解决争端最权威的信息源泉，它成功地记录了各种英勇事迹、超常行为、耐力表演等. 而这些记录反过来又影响和激发了更多人做同样的尝试. 于是人们会看到，双人舞无休止地进行、有人和蛇一起呆在棺材里. 这些活动周而复始地举行，只是为了在这本记录琐事的圣经中留下自己的名字. 书中也有体育记录以及身高体重和生育等方面的超常事实等.

在这本书中很少记录科学领域的事情. 事实上，科学家尤其是数学家在酒吧里喝红酒或啤酒时也很喜欢聊天. 在喝了一阵之后，也会对诸如关于新发现的某种数等各样最新记录打赌.

老实说，假如我在《辉格标准报》中能够读到，人们在公众场合的吵架是源于对目前已知的最大孪生素数对的激烈争辩，我会觉得这种吵架更文明一些.

但是，不是每个人都认为人们之间的争斗是所希望的，即使这种争斗有很重要的理由. 所以，我想揭示某些记录. 任何人若是知道更好的记录，请把新的信息告诉我.

我只讨论素数：它们是一些自然数 2,3,5,7,11,··· 它们不会被任何比它小的自然数 (除了 1 之外) 除尽. 若自然数不是 1 也不是素数，则叫作合成数.

素数是重要的，因为算术基本定理说，每个大于 1 的自然数均是素数的乘积，并且这种分解本质上是唯一的.

“哪个素数是特别的？” 不用说，这是一个很容易回答的问题：是素数 2, 因为它是偶素数！

遇到素数的机会 (例如 1093 和 608981813029) 并不大，它们有各种有趣的性质. 素数彼此很像表姐妹，她们是同一家族的成员，彼此长得很像，但又不完全一样.

在讲述关于素数的各种记录的时候，我首先遇到的问题是如何组织这些材料. 也就是说，对于素数理论的研究和发展如何分成几条主线.

一般来说，在研究某个数集 (我们这里是素数集合) 的时候，会问到下列一些问题：该集合有多少数？如何决定任意一个数是否属于这个数集？如何描述这些数？这种数在绝对值很大时或在小区间中分布如何？然后便集中注意这种数的各种类型，同时对这些数做各种试验，于是像其他科学领域中那样提出一些猜测.

按这种方式，我们把素数问题分成以下几个专题：

(1) 素数有多少？

(2) 如何识别一个自然数是否为素数？

(3) 是否存在定义素数的一些函数？

(4) 素数的分布如何？

(5) 哪些素数的特殊性质需要考虑？

(6) 关于素数的实验和概率统计结果.

在讨论这些问题时我们将提供素数的有关记录.



数 学 符 号

符号	含义
$m \mid n$	整数 m 整除整数 n
$m \nmid n$	整数 m 不能整除整数 n
$p^e \parallel n$	p 是素数， $p^e \mid n$ 但 $p^{e+1} \nmid n$
$\gcd(m, n)$	整数 m, n 的最大公因子
$lcm(m, n)$	整数 m, n 的最小公倍数
$\log(x)$	实数 $x > 0$ 的自然对数
$\mathbb{Z}$	整数环
$\mathbb{Q}$	有理数域
$\mathbb{R}$	实数域
$\mathbb{C}$	复数域

下面列出在书中出现的符号

符号	含义
p_n	第 n 个素数
$p\#$	小于 p 的所有素数的乘积，或叫 p 的素连乘
F_n	第 n 个费马数， $F_n = 2^{2^n} + 1$
$[x]$	x 的整数部分，即满足 $[x] \leqslant x \leqslant [x] + 1$ 的唯一整数 $[x]$
g_p	模 p 的最小原根
$\varphi(n)$	欧拉函数
$\lambda(n)$	Carmichael 函数
$\omega(n)$	n 的不同素因子个数
$L(x)$	$n \leqslant x$ 且 $\varphi(n)$ 整除 $n-1$ 的合成数 n 的个数

符号	含义
$V_\psi(m)$	$\#\{n \geqslant 1 \mid \varphi(n) = m\}$
t_n^*	$a^n - b^n$ 的主要部分
$k(m)$	m 的无平方因子
$P[m]$	m 的最大素因子
S_r	至多有 $r \log\log n$ 个不同素因子的整数 n 全体
$\left(\dfrac{a}{p}\right)$ 或 $(a \mid p)$	Legendre 符号
$\left(\dfrac{a}{b}\right)$ 或 $(a \mid b)$	Jacobi 符号
$U_n = U_n(P,Q)$	参数为 (P,Q)Lucas 序列的第 n 项
$V_n = V_n(P,Q)$	参数为 (P,Q)Lucas 序列的第 n 项
$\rho(n) = \rho(n,U)$	n 能整除 U_r 的最小 r
$\psi(p)$	$= p - (D \mid p)$
$\left(\dfrac{\alpha,\beta}{p}\right)$	与 $X^2 - PX + Q$ 的两个根 α,β 有关的符号
$\psi_{\alpha,\beta}(p)$	$= p - \left(\dfrac{\alpha,\beta}{p}\right)$ 其中 p 是奇素数
$\psi_{\alpha,\beta}(p^e)$	$= p^{e-1}\psi_{\alpha,\beta}(p)$ 其中 p 是奇素数
$\lambda_{\alpha,\beta}\left(\prod p^e\right)$	$lcm\{\psi_{\alpha,\beta}(p^e)\}$
$\mathcal{P}(U)$	整除某项 $U_n \neq 0$ 的素数全体
$\mathcal{P}(V)$	整除某项 $V_n \neq 0$ 的素数全体
U_n^*	U_n 的本原部分
$\psi_D\left(\prod_{i=1}^s p_i^{e_i}\right)$	$= \dfrac{1}{2^{s-1}} \displaystyle\prod_{i=1}^{s} \left(p_i^{e_i-1} - \left(p_i - \left(\dfrac{D}{p_i}\right)\right)\right)$
Pn	有 n 位数字的素数
Cn	有 n 位数字的合成数
M_q	$= 2^q - 1$， Mersenne 数

符号	含义
$\sigma(n)$	n 的因子之和
$\tau(n)$	n 的因子个数
$H(n)$	n 的因子的调和平均
$V(x)$	x 以内完全数的个数
$s(n)$	n 的真因子之和
psp	以 2 为基的拟素数
$\mathrm{psp}(a)$	以 a 为基的拟素数
$B_{\mathrm{psp}}(n)$	$\#\{a\|1 < a \leqslant n-1, \gcd(a,n)=1, n$为 $\mathrm{psp}(a)\}$
$\mathrm{epsp}(a)$	以 a 为基的欧拉拟素数
$B_{\mathrm{epsp}}(n)$	$\#\{a\|1 < a \leqslant n-1, \gcd(a,n)=1, n$为 $\mathrm{epsp}(a)\}$
$\mathrm{spsp}(a)$	以 a 为基的强欧拉拟素数
$B_{\mathrm{spsp}}(n)$	$\#\{a\|1 < a \leqslant n-1, \gcd(a,n)=1, n$为 $\mathrm{spsp}(a)\}$
$M_3(m)$	$=(6m+1)(12m+1)(18m+1)$
$M_k(m)$	$=(6m+1)(12m+1)\prod_{i=1}^{k-2}(9\times 2^i m+1)$
C_k	如果 $1 < a \leqslant n-1, \gcd(a,n)=1$，则 $a^{n-k} \equiv 1(mod\ n)$. 满足上述条件且大于 k 的合成数 n 全体 (当 $k>1$ 时为 Knödel 数)
$\mathrm{lpsp}(P,Q)$	具有参数 (P,Q) 的 Lucas 拟素数
$B_{\mathrm{lpsp}}(n,D)$	$\#\{1 < P \leqslant n$ 存在Q, 使得$D \equiv P^2-4Q\ (mod\ n)$ 为 $\mathrm{lpsp}(P,Q)\}$
$elpsp(P,Q)$	具有参数 (P,Q) 的 Euler-Lucas 拟素数
$slpsp(P,Q)$	具有参数 (P,Q) 的强 Lucas 拟素数
$\pi(x)$	小于 x 的素数个数
$\mu(x)$	Möbius 函数
Δ	与 $d \neq 0,1$ 结合的基本判別式

符号	含义
$\mathbb{Q}(\sqrt{d})$	$=\mathbb{Q}(\sqrt{\Delta})$，二次域
Cl_d或Cl_Δ	$\mathbb{Q}(\sqrt{d})$ 的类群
h_d或h_Δ	$\mathbb{Q}(\sqrt{d})$ 的类数
e_d	Cl_d 类群的指数
$\pi^*_{f(X)}(N)$	$\#\{n \mid 0 \leqslant n \leqslant N, \lvert f(n)\rvert$是素数$\}$
$P_0[m]$	$m>1$ 的最小素因子
$P_0[f(X)]$	$\min\{P_0[f(X)] \mid k=0,1,2,\cdots\}$
$f(x)\sim h(x)$	f,h 渐近相等
$f(x)=g(x)+O(h(x))$	差 $f(x)-g(x)$ 以 $h(x)$ 的常数倍数为上界
$f(x)=g(x)+o(h(x))$	差 $f(x)-g(x)$ 与 $h(x)$ 比较可忽略不计
$\zeta(s)$	黎曼 Zeta 函数
B_k	Bernoulli 数
$S_k(n)$	$=\sum_{j=1}^{n} j^k$
$B_k(X)$	Bernoulli 多项式
$Li(x)$	对数积分
$\theta(x)$	$=\sum_{p\leqslant x}\log p$, Tschebycheff 函数
$Re(s)$	s 的实数部分
$\Gamma(s)$	Gamma 函数
γ	欧拉常数
$J(x)$	加权的素数幂计算函数
$R(x)$	黎曼函数
$\Lambda(x)$	van Mangoldt 函数
$\varphi(x)$	van Mangoldt 函数的求和函数
$M(x)$	Mertens 函数
$\varphi(x,m)$	$\#\{a \mid 1\leqslant a\leqslant x, a$不是$1,2,\cdots,p_m$倍数$\}$

符号	含义
ρ_n	zeta 函数在临界区域的上半平面部分的第 n 个非平凡零点
$N(T)$	$\#\{\rho=\sigma+it \mid 0\leqslant\sigma\leqslant 1, \varsigma(\rho)=0, 0<t\leqslant T\}$
d_n	$=p_{n+1}-p_n$
$g(p)$	大于 p 的连续合成数的个数
G	$=\{m \mid 对某个p>2, m=g(p)\}$
$p[m]$	使得 $g(p)=m$ 的最小素数 p
$\log_2 x$	$\log\log x$
$\log_3 x$	$\log\log\log x$
$\log_4 x$	$\log\log\log\log x$
B	Brun 常数
$\pi_2(x)$	$\#\{素数p \mid p+2\leqslant x且p+2也是素数\}$
C_2	$=\prod_{p>2}\left(1-\frac{1}{(p-1)^2}\right)$，孪生素数常数
$\pi_{2k}(x)$	$\#\{n\geqslant 1 \mid p_n\leqslant \; and \; p_{n+1}-p_n=2k\}$
$\pi_{2,6}(x)$	$\#\{素数p \mid p\leqslant x且p+2, p+6也是素数\}$
$\pi_{4,6}(x)$	$\#\{素数p \mid p\leqslant x且p+4, p+6也是素数\}$
$\pi_{2,6,8}(x)$	$\#\{素数p \mid p\leqslant x且p+2, p+6, p+8 \text{ 也是素数 }\}$
$B_{2,6}$	$=\sum\left(\frac{1}{p}+\frac{1}{p+2}+\frac{1}{p+6}\right)$ 在所有素数三元组 $(p,p+2,p+6)$ 上求和
$B_{4,6}$	$=\sum\left(\frac{1}{p}+\frac{1}{p+4}+\frac{1}{p+6}\right)$ 在所有素数三元组 $(p,p+4,p+6)$ 上求和
$B_{2,6,8}$	$=\sum\left(\frac{1}{p}+\frac{1}{p+2}+\frac{1}{p+6}+\frac{1}{p+8}\right)$ 在所有素数四元组 $(p,p+2,p+6,p+8)$ 上求和
$\rho^*(x)$	$=k$表示存在允许的 $(k-1)$- 数组 $b_1, b_2, \cdots, b_{k-1}$ 使得 $b_{k-1}<x$ 但是不存在多于 $k-1$ 个分量的

符号	含义
	这种数组
$\rho(x)$	$= \limsup_{y\to\infty}(\pi(x+y)-\pi(y))$
$\pi_{d,a}(x)$	$\#\{$素数$p \mid p \leqslant x, p \equiv a(mod\ d)\}$
$p(d,a)$	在算术级数 $\{a+kd \mid k \geqslant 0\}$ 中最小的素数
$p(d)$	$= \max\{p(d,a) \mid 1 \leqslant a < d, \gcd(a,d)=1\}$
L	Linnik 常数
P_k	k 殆素数集合
S, S_0	Schnirelmann 常数
$r_2(2n)$	$2n$ 表示成两个素数和的方法数
$G'(n)$	$\#\{2n \mid 2n \leqslant x, 2n$不是两个素数和$\}$
$(psp)_n$	第 n 个拟素数
$P\pi(x)$	小于等于 x 的基为 2 的拟素数的个数
$P\pi_a(x)$	小于等于 x 的基为 a 的拟素数的个数
$EP\pi(x)$	小于等于 x 的基为 2 的欧拉拟素数的个数
$EP\pi_a(x)$	小于等于 x 的基为 a 的欧拉拟素数的个数
$SP\pi(x)$	小于等于 x 的基为 2 的强拟素数的个数
$SP\pi_a(x)$	小于等于 x 的基为 a 的强拟素数的个数
$l(x)$	$= \mathrm{e}^{\log x \log\log\log x / \log\log x}$
$psp(d,a)$	$\gcd(a,d)=1$，在算术级数 $\{a+kd \mid k \geqslant 0\}$ 中最小的拟素数
$CN(x)$	$\#\{n \mid 1 \leqslant n \leqslant x, n$是 Carmichael 数$\}$
$L\pi(x)$	具有 (P,Q) 参数且小于等于 x 的 Lucas 拟素数个数
$SL\pi(x)$	具有 (P,Q) 参数且小于等于 x 的 Lucas 强拟素数个数

符号	含义
ς_p	$=\cos(2\pi/p)+\mathrm{i}\sin(2\pi/p)$
$h(p)$	第 p 个分圆域的类数
$\pi_{reg}(x)$	$p\leqslant x$ 的正规素数的个数
$\pi_{ir}(x)$	$p\leqslant x$ 的非正规素数的个数
$ii(p)$	p 的不正规指数
$\pi_{iis}(x)$	满足 $p\leqslant x, ii(p)=s$ 的素数 p 的个数
$S_{d,a}(x)$	$\#\{p\text{是素数}\mid p\leqslant x, dp+a\text{是素数}\}$
$q_p(a)$	$=\frac{a^{p-1}-1}{p}$， p 的基为 a 的费马商
$W(p)$	$=\frac{(p-1)!+1}{p}$， Wilson 商
Rn	$\frac{10^n-1}{9}$
Cn	$=n\times 2^n+1$， Cullen 数
$C\pi(x)$	$\#\{n\mid C_n\leqslant x\text{且}C_n\text{是素数}\}$
Wn	$=n\times 2^n-1$， Woodall 数或第二类 Cullen 数
$\mathcal{P}(T)$	整除序列 $T=(T_n)_{n\geqslant 0}$ 中某项的素数全体
$\pi_H(x)$	$\#\{p\in P(H)\mid p\leqslant x\}$
S_{2n+1}	NSW 数
$\pi_{f(X)}(x)$	$\#\{n\geqslant 1\mid \|f(n)\|\leqslant x\text{且}\|f(n)\|\text{是素数}\}$
$p(f)$	使得 $\|f(m)\|$ 是素数的最小整数 $m\geqslant 1$
$\pi_{X,X+2k}(x)$	$\#\{\text{素数}p\mid p+2k\text{是素数且}p+2k\leqslant x\}$
$\pi_{X^2+1}(x)$	$\#\{\text{素数}p\mid \text{要求}p=m^2+1, p\leqslant x\}$
$\pi_{aX^2+bX+c}(x)$	$\#\{\text{素数}p\mid \text{要求}p=am^2+bm+c, p\leqslant x\}$

目　　录



第一章　素数有多少？

这个问题的答案是下列基本定理：

素数有无穷多个.

我将给出这个定理的七个证明 (再加上这些证明的四个变种)，这些证明均由著名数学家给出，其中有些数学家已被人遗忘. 其中一些证明引发出有趣的新发展，另一些证明也很聪明和巧妙. 当然还有更多的关于素数无穷的证明 (当然没有无穷多个证明).

1.1　欧几里得 (Euclid) 的证明

假设 $p_1 = 2 < p_2 = 3 < \cdots < p_r$ 是全部素数，令 $P = p_1p_2\cdots p_r+1$, 并且 p 为除尽 P 的一个素数, 则 p 不能是 $p_1, p_2, \cdots, p_r$ 当中的任何一个. 因为否则，将除尽差数 $P - p_1p_2\cdots p_r = 1$, 而这是不可能的. 所以 p 又是一个新的素数，从而 $p_1, p_2, \cdots, p_r$ 不能为全部素数. □

我们把素数按递增的顺序写成一个序列

$$p_1 = 2,\ p_2 = 3,\ p_3 = 5,\ p_4 = 7,\ \cdots,\ p_n,\ \cdots$$

1878 年，库默尔 (Kummer) 给出欧几里得证明的一个巧妙的新形式.

库默尔的证明　假设只有有限多个素数 $p_1 < p_2 < \cdots < p_r$. 令 $N = p_1p_2\cdots p_r > 2$, 则整数 $N-1$ 为一些素数的乘积，从而必有某个 p_i 为 N 的素因子，于是 p_i 除尽 $N-(N-1) = 1$, 这又推

出矛盾！ □

由杰出数学家给出的这个证明像珍珠那样圆润、光亮，并且有简洁的美.

另一个伟大的数学家斯蒂尔吉斯 (Stieltjes) 在 1890 年给出一个类似于库默尔的证明.

你是否喜欢库默尔的证明？你再与下面一个证明比较一下，这是一个更漂亮和更简单的证明．这个证明是纳吉维奇(W.Narkiewitz) 告诉我的，它发表于 1915 年《Intermédiaire des Mathématiques》第 22 卷第 253 页，文章作者为布洛卡德 (H. Brocard), 但是他说这个证明是厄米特 (Harmite) 给出的．它当然也可看成是欧几里得证明的又一种形式.

我们只需证明：对每个自然数 n, 必存在大于 n 的素数．为此考虑 $N!+1!$ 的一个素因子即可达到目的 (如果你不喜欢第二个惊叹号，可以把 1! 写成 1).

欧几里得的证明非常简单，但是在每个阶段都没有给出新的素数的任何信息，只是说这个新素数不超过 $P = p_1p_2\cdots p_n + 1$. 所以 P 本身可能是素数 (对某些 n), 也可能是合成数 (对另一些 n).

对每个素数 p, 我们用 $p\#$ 表示不超过 p 的所有素数 q 的乘积．根据都伯纳 (Dubner) 于 1987 年的建议， $p\#$ 叫作 p 的素连乘 (primorial).

下列两个问题至今均不知道答案：

是否有无穷多素数 p, 使得 $p\#+1$ 为素数？

是否有无穷多素数 p, 使得 $p\#+1$ 为合成数？

记录 形如 $p\#+1$ 的至今已知最大素数为

Caldwell 和 Gallot(2002) 对于所有 $p < 120000$ 试验，发现当

且仅当 p=2, 3, 5, 7, 11, 31, 379, 1019, 1021, 2657, 3229, 4547, 4787, 11549, 13649, 18523, 23801, 24029, 42209 时，$p\#+1$ 为素数. 在这之前的工作可见 Borning(1972),Templer(1980),Buhler, Crandall 与 Penk(1982), Caldwell 与 Dubner(1993),Caldwell(1995).

素　数	十进制位数	发现时间	发 现 人
$392113\#+1$	169966	2001	D.Heuer 等人
$366439\#+1$	158936	2001	D.Heuer 等人
$145823\#+1$	63142	2000	D.E.Robinson 等人

人们也研究了形如 $p\#-1$ 的数是否为素数？在 Caldwell 和 Gallot 的文章中报告：对于 $p<120000$, 当且仅当 p=3, 5, 11, 13, 41, 89, 317, 337, 991, 1873, 2053, 2377, 4093, 4297, 4583, 6569, 13033, 15877 时，$p\#-1$ 为素数.

欧几里得的证明还引发出其他问题. 例如，考虑序列 $q_1=2, q_2=3$, $q_3=7$, $q_4=43$, $q_5=139$, $q_6=50207$, $q_7=340999$, $q_8=2365347734339, \cdots$ 其中 q_{n+1} 是 $q_1q_2\cdots q_n+1$ 的最大素因子 (从而 $q_{n+1}\neq q_1,q_2,\cdots,q_n$). Mullin 于 1963 年问：序列 $(q_n)_{n\geqslant 1}$ 是否包含所有素数？是否只有有限多个素数不在此列？这个序列是否单调递增？

关于第一个问题，容易看出 5 不在这个 Mullin 序列之中. 1968 年，Cox 和 van der Poorten 发现了一个给定素数不属于此序列的充分性同余式判别法. 用这种方法，他们证明了：对于不超过 47 的素数，只有 2, 3, 7, 43 不属于 Mullin 序列. 证明细节可见 Narkiewitz(2000) 的书.

关于第二个问题，人们倾向于认为有无穷多素数不属于 Mullin 序列. 对于最后一个问题，Naur 于 1984 年将前人的计算加以扩

展，证明了 $q_{10} < q_9$, 所以 $(q_n)_{n\geqslant 1}$ 不是单调递增的.

1991 年， Shanks 考虑一个类似的序列： $l_1 = 2, l_2 = 3, l_3 = 7, l_4 = 43, l_5 = 13, l_6 = 53, l_7 = 5$, $l_8 = 6221271, \cdots$ 一般地， l_{n+1} 是 $l_1 l_2 \cdots l_n + 1$ 的最小素因子. Shanks 猜想每个素数均属于这个序列，但至今不知这是否正确. Wagstaff(1993) 对 $n \leqslant 43$ 计算出所有 l_n, 推广了 Guy 和 Nowakowski(1975) 的计算.

这些序列诸项的计算需要决定最小素因子，或者要把相当大的数进行因子分解. 当数增大时做这件事情越来越困难. 我们将在第二章第 2.11D 节讨论因子分解问题.

1985 年， Odoni 考虑一个类似的序列

$$w_1 = 2, w_2 = 3, \cdots, w_{n+1} = w_1 w_2 \cdots w_n + 1$$

他证明了:存在无穷多个素数不是此序列中任何一项的因子. 当然，也存在无穷多个素数至少是序列中某项的因子.

1.2 哥德巴赫 (Goldbach) 也有证明！

这个证明的思想很简单，但富有成果. 我们只需要找到一个自然数的无穷序列 $1 < a_1 < a_2 < a_3 < \cdots$, 使任意两项均互素 (即没有公共素因子). 因为对于这种序列，令 p_1 为 a_1 的素因子， p_2 为 a_2 的素因子，如此下去，则 $p_1, p_2, \cdots$ 彼此不同.

证明关键在于，最大公因子可以用辗转相除法求得，不需要这些数的素因子知识.

对于一个好的想法，特别是它很简单的时候，很难确定谁是首先有此想法的. 我曾认为这个思想来自 Pólya 和 Szegö(见他们 1924 年的书).E.Specker 让我注意到：Pólya 用了 Hurwitz(1891) 的一个习题. 而 W.Narkiewitz 又告诉我，哥德巴赫在给欧拉的信中

(1730 年 7 月 20~31 日), 写了下面用费马数的证明，这也许是哥德巴赫写出的唯一的证明.

费马数 $F_n = 2^{2^n} + 1 (n \geqslant 0)$ 彼此互素.

证明 对 m 做归纳法可知 $F_m - 2 = F_0 F_1 \cdots F_{m-1}$. 所以当 $n < m$ 时， F_n 除尽 $F_m - 2$.

如果素数 p 同时除尽 F_n 和 F_m, 则它必是 $F_m - 2$ 和 F_m 的公因子，从而 $p = 2$. 但是 F_n 为奇数，从而不可被 2 除尽. 这表明费马数是彼此互素的. □

前五个费马数为 $F_0 = 3, F_1 = 5, F_2 = 17, F_3 = 257$ 和 $F_4 = 65537$. 容易验证它们都是素数. F_5 是 10 位数，并且以后每个费马数都差不多是前一个费马数的平方，所以增长得很快. 一个重要的问题是：哪些 F_n 是素数或至少求出 F_n 的一个素因子. 我将在第二章回到这个问题.

希望能发现其他无穷序列，使任两项均互素，并且构作这个序列时不利用素数无穷的性质. Edward 于 1964 年考虑了这个问题，用递归方式定义了一些序列具有上述性质. 例如，若 $S_0 = 3$ 和 a 是互素的整数， $S_0 > a \geqslant 1$, 则由递归关系

$$S_n - a = S_{n-1}(S_{n-1} - a) \quad (n \geqslant 1)$$

给出自然数序列其中任意两项均互素. 当 $S_0 = 3, a = 2$ 时就给出费马数 $S_n = F_n = 2^{2^n} + 1$.

类似地取 S_0 为奇数而

$$S_n = S_{n-1}^2 - 2 \quad (n \geqslant 1)$$

则整数序列 S_n 也是两两互素的. 这个序列由 Lucas 所考虑，我也在第二章再回到这个序列.

1947 年， Bellman 给出下述方法，不用素数无穷性，构作彼此互素的无穷序列．先取一个整系数多项式 $f(X), f(0) \neq 0, f(x)$ 不恒为常数，并且若 n 和 $f(0)$ 互素，则 $f(n)$ 和 $f(0)$ 必互素．然后令

$$f_1(X) = f(X), \quad f_{m+1}(X) = f(f_m(X)) \quad (m \geqslant 1)$$

如果对每个 $m \geqslant 1$ 均有 $f_m(0) = f(0)$, 并且 n 和 $f(0)$ 互素，则整数 $n, f_1(n), f_2(n), \cdots, f_m(n), \cdots$ 必然两两互素．例如，$f(X) = (X-1)^2 + 1$ 满足上述条件，而 $f_n(-1) = 2^{2^n} + 1$, 于是又回到费马数！

P.Schorn 告诉我证明素数无穷多的下一个方法, 它是 Hurwitz 想法的一个变种．

Schorn 的证明 首先注意：对于 $1 \leqslant i < j \leqslant n$, 则

$$\gcd((n!)i + 1, (n!)j + 1) = 1$$

事实上，令 $j = i + d, 1 \leqslant d \leqslant n$, 则 $(n!)d$ 的素因子均不超过 n. 所以

$$\gcd((n!)i + 1, (n!)j + 1) = \gcd((n!)i + 1, (n!)d) = 1$$

再设素数共有 m 个, 令 $n = m+1$, 则由上面的事实可知 $m+1$ 个整数 $(m+1)!i + 1$ $(1 \leqslant i \leqslant m+1)$ 两两互素，从而至少存在 $m+1$ 个素数，这与假设矛盾． □

1.3 欧拉 (Euler) 的证明

这是一个间接的证明．在某种意义上说，这个证明是不自然的．但是另一方面，我将指出，这个证明引发出很重要

的数学发展.

欧拉证明素数无穷多，是由于所有素数的某个表达式的值为无穷大.

对于每个素数 p, $\frac{1}{p} < 1$. 于是有几何级数求和

$$\sum_{k=0}^{\infty} \frac{1}{p^k} = \frac{1}{1 - \frac{1}{p}}$$

类似地，对另一个素数 q

$$\sum_{k=0}^{\infty} \frac{1}{q^k} = \frac{1}{1 - \frac{1}{q}}$$

将这两个等式相乘

$$1 + \frac{1}{p} + \frac{1}{q} + \frac{1}{p^2} + \frac{1}{pq} + \frac{1}{q^2} + \cdots = \frac{1}{1 - \frac{1}{p}} \cdot \frac{1}{1 - \frac{1}{q}}.$$

左边是所有自然数 $p^h q^k (h, k \geqslant 0)$ 的倒数之和，由唯一因子分解定理知这些自然数不重复. 这个简单想法是证明的基础.

欧拉的证明 设 $p_1, p_2, \cdots, p_n$ 是素数全体，则

$$\sum_{k=0}^{\infty} \frac{1}{p_i^k} = \frac{1}{1 - \frac{1}{p_i}} \quad (1 \leqslant i \leqslant n)$$

将这 n 个等式相乘，得到

$$\prod_{i=1}^{n} \left(\sum_{k=0}^{\infty} \frac{1}{p_i^k} \right) = \prod_{i=1}^{n} \frac{1}{1 - \frac{1}{p_i}}$$

左边是所有自然数的倒数和，由算术基本定理，每个自然数恰好出现一次. 但是级数 $\sum_{n=1}^{\infty} \frac{1}{n}$ 是发散的，而上式左边有限，这导致矛盾.

我在第四章要讲这个证明引伸出的数学发展.

1.4 Thue 的证明

Thue 的证明只用自然数唯一因子分解的基本定理.

Thue 的证明 先取整数 $n, k \geqslant 1$, 并且 $(1+n)^k < 2^n$. 令 $p_1 = 2, p_2 = 3, \cdots, p_r$ 是不超过 2^n 的全部素数. 假设 $r \leqslant k$, 由基本定理知每个整数 $m (1 \leqslant m \leqslant 2^n)$ 唯一表成

$$m = 2^{e_1} 3^{e_2} \cdots p_r^{e_r} \quad (0 \leqslant e_1, e_2, \cdots, e_r \leqslant n)$$

计算所有的可能性, 给出 $2^n \leqslant (n+1)n^{r-1} < (n+1)^r \leqslant (n+1)^k < 2^n$. 这个矛盾表明 $r \geqslant k+1$.

取 $n = 2k^2$, 由 $1 + 2k^2 < 2^{2k}$(对每个 $k \geqslant 1$) 可知

$$(1+2k^2)^k \leqslant 2^{2k^2} = 4^{k^2}$$

所以至少有 $k+1$ 的素数 p 满足 $p < 4^{k^2}$. 由于 k 可任意大，这就证明了素数有无穷多个. □

这个证明是说，$k+1$ 是超不过 4^{k^2} 的素数个数的一个下界. 这是一个定量的结果，这个下界当然很粗. 在第四章我将进一步研究这类问题.

1.5 三个被遗忘的证明

下面三个证明分别由 Perott,Auric 和 Métrod 给出. 谁知道这些人的名字? 如果没有 Dickson 的《数论史》一书, 他们会被后人完全遗忘. 这些证明均很巧妙和令人喜欢, 但是都没有给数学以新的视野.

Perott 的证明 这个证明是 1881 年给出的. 它利用级数 $\sum\limits_{n=1}^{\infty}\dfrac{1}{n^2}$ 是收敛的, 并且其和值小于 2(根据欧拉的著名结果, 这个和式的值为 $\pi^2/6$, 我将在第四章回到此). 事实上

$$\sum_{n=1}^{\infty}\frac{1}{n^2}<1+\sum_{n=1}^{\infty}\frac{1}{n(n+1)}=1+\sum_{n=1}^{\infty}\left(\frac{1}{n}-\frac{1}{n+1}\right)=1+1=2$$

假设只有 r 个素数 $p_1<p_2<\cdots<p_r$. 取自然数 N 使得 $p_1\cdots p_r<N$, 则不被平方数除尽的整数 $m<N$ 共有 2^r 个 (2^r 是不同素数乘积的个数). 被 p_i^2 除尽的 $m(<N)$ 最多有 N/p_i^2 个. 所以被某个平方数除尽的 $m(<N)$ 最多有 $\sum_{i=1}^{r}N/p_i^2$ 个. 于是

$$N\leqslant 2^r+\sum_{i=1}^{r}\frac{N}{p_i^2}<2^r+N\left(\sum_{n=1}^{\infty}\frac{1}{n^2}-1\right)=2^r+N(1-\delta)$$

其中 $\delta>0$. 取 N 使得 $N\delta\geqslant 2^r$, 则给出矛盾. □

Auric 的证明 这个证明做于 1915 年, 非常简单.

假设只有 r 个素数 $p_1<p_2<\cdots<p_r$. 取任一整数 $t\geqslant 1$, 记 $N=p_r^t$. 由唯一因子分解定理, 对每个整数 m,$1\leqslant m\leqslant N$, 记 $m=p_1^{f_1}p_2^{f_2}\cdots p_r^{f_r}$, 则 $(f_1,f_2,\cdots,f_r)(f_i\geqslant 0)$ 由 m 所决定. 由于 $p_1^{f_i}\leqslant p_i^{f_i}\leqslant m\leqslant N=p_r^t$. 可知对 $1\leqslant i\leqslant r$, $f_i\leqslant tE$, 其中 $E=(\lg p_r)/(\lg p_1)$. 于是 $m(1\leqslant m\leqslant N)$ 的个数 N 不超过

$(f_1, f_2, \cdots, f_r)$ 的个数，即 $p_r^t = N < (tE+1)^r < t^r(E+1)^r$. 当 t 充分大时，这个不等式是不能成立的. 由此证明了素数有无穷多个. □

Métrod 的证明 这个证明做于 1917 年，也很简单.

假设只有 r 个素数 $p_1 < p_2 < \cdots < p_r$. 记 $N = p_1p_2\cdots p_r$, 对每个 $1 \leqslant i \leqslant r$, 令 $Q_i = N/p_i$, 则对每个 i, p_i 除不尽 Q_i, 而当 $j \neq i$ 时， p_i 除尽 Q_j. 令 $S = \sum_{i=1}^{r} Q_i$. 如果 q 是 S 的素因子，则 $q \neq p_i$, 因为 p_i 除尽 $Q_j (j \neq i)$ 但是除不尽 Q_i, 这表明存在新的素数！ □

1.6 Washington 的证明

这个证明 (1980) 要用交换代数中关于主理想整环、唯一分解整环、Dedekind 整环和代数数论的一些基本知识，这些知识可见这方面的任何一本教科书，如 Samuel(1967) 的书. 这些知识并不十分深奥. 下面列举我们所需要的一些事实.

(1) 每个数域 (有理数域的有限次扩张域) 的代数扩张的代数整环都是 Dedekind 整环，即每个非零素理想都唯一表示成素理想的乘积.

(2) 每个数域中必有有限多个素理想除尽任何给定的素数 p.

(3) 只有有限多个素理想的 Dedekind 整环必是主理想整环，并且每个非零元素 (不计单位因子) 均唯一表示成素元素的乘积.

Washington 的证明 考虑全体形如 $a + b\sqrt{-5}$ (a, b 为有理数) 的数组成的数域. 这个域的整数环是由 $a + b\sqrt{-5}$ (a, b 为通常整数) 所组成的. 不难看出 $2, 3, 1+\sqrt{-5}, 1-\sqrt{-5}$ 均是这个整数

环中的素元，因为它们均不能再分解成一些代数整数因子之积，使得每个因子均不为单位元素 ± 1. 注意

$$(1+\sqrt{-5})(1-\sqrt{-5}) = 2 \times 3$$

是 6 的两种本质上不同的素元分解，所以这个整数环不是唯一分解整环. 于是它一定有无穷多个素理想 (根据上面的事实 (3)). 然后可知有无穷多个素数 (根据上面的事实 (2)).

1.7 Furstenberg 的证明

这个巧妙的证明使用拓扑学的思想，因为它很短，最好我直接引用 1955 年文章中的原文：

在这篇短文中我们将对于素数无穷性给出一个初等的“拓扑”证明. 我们在整数集合 S 中，取所有算术级数 $(-\infty \sim +\infty)$ 的基，S 可成为一个拓扑空间. 事实上，对于这个拓扑，可以证明 S 是正则空间，并且是可距离化的. 每个算术级数是又开又闭的集合，因为它的补集是具有用样公差的其他算术级数的并，于是，任意有限个算术级数的并也是闭集.

对素数 p，令 A_p 是 p 的全部倍数组成的集合. 现在考虑集合 $A = \bigcup_p A_p$，其中 p 过全部素数. 则只有 ± 1 是不在 A 中的整数. 由于 $1, -1$ 显然不是开集，从而 A 不是闭集. 这表明素数有无穷多个.

Golomb 将 Furstenberg 的想法加以发展，于 1959 年写了一篇有趣的短文.

第二章　如何识别一个自然数是否为素数

高斯在《算术探究》(1801) 一书的 329 页中写到：

把素数和合成数区分开来和把合成数分解出素因子是算术中最重要和有益的问题之一 …… 科学本身的自尊要求人们采用一切可能的手段来探索去解决这个如此精美和著名的问题.

对于素性和分解问题的第一步考察是清楚的：这两件事都有算法. 我指的是存在一个只包含有限步的程序，它用到任何数 N 上，都能指明 N 是否为素数，或者当 N 是合成数时给出它的所有素因子. 也就是说，给了自然数 N, 依次对 $n = 2, 3, \cdots$ 直到 $[\sqrt{N}]$(不超过 $\sqrt{N}$ 的最大整数) 去试 n 是否整除 N. 如果这些 n 均不整除 N, 则 N 为素数. 如果某个 N_0 整除 N, 则 $N = N_0N_1$, 从而 $N_1 < N$. 再对 N_0 和 N_1 重复上述程序，最终给出 N 的素因子完全分解.

我上面讲的事情，似乎浅显得无话可说了. 但是要注意，对于大数 N 用上述算法来决定 N 是否为素数，可能会花很长时间.

这就触及到最重要的实际方面：需要寻求一个有效的算法，使它包含尽可能少的运算，从而实现起来花费最少的时间和财力.

我打算把本章分成几节，分别审视不同的方法和解释所需的理论结果.

2.1　Eratosthenes 筛法

我前面说过，如果用不超过 $\sqrt{N}$ 的每个 n 去试除 N, 就可决

定 N 是否为素数. 由于乘法比除法运算更容易, Eratosthenes(公元前三世纪) 想出一个计算方法, 就是著名的筛法. 对于给定的任何 N, 用此法均可决定 N 以内的所有素数以及合成数的因子分解. 现在用 $N = 101$ 来说明这个方法.

把从 2 到 101 的数依次写下来, 划去所有 2 的倍数但是留下 2. 以后每一步, 对于剩下数中的最小数 p, 划去 p 的所有倍数但是留下 p. 一直做到 $p^2 < 101$ 时为止.

这样一来, 不超过 $\sqrt{101}$ 的 $2, 3, 5, 7, \cdots$ 的倍数都被划掉, 53 为素数因为它没有被拿走. 所以 101 以内的素数为 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97, 101.

这个程序是筛法的基础, 它已被大大地推广, 用来估计满足一些给定条件的素数个数.

	2	3	~~4~~	5	~~6~~	7	~~8~~	~~9~~	~~10~~
11	~~12~~	13	~~14~~	~~15~~	~~16~~	17	~~18~~	19	~~20~~
~~21~~	~~22~~	23	~~24~~	~~25~~	~~26~~	~~27~~	~~28~~	29	~~30~~
31	~~32~~	~~33~~	~~34~~	~~35~~	~~36~~	37	~~38~~	~~39~~	~~40~~
41	~~42~~	43	~~44~~	~~45~~	~~46~~	47	~~48~~	~~49~~	~~50~~
~~51~~	~~52~~	53	~~54~~	~~55~~	~~56~~	~~57~~	~~58~~	59	~~60~~
61	~~62~~	~~63~~	~~64~~	~~65~~	~~66~~	67	~~68~~	~~69~~	~~70~~
71	~~72~~	73	~~74~~	~~75~~	~~76~~	~~77~~	~~78~~	79	~~80~~
~~81~~	~~82~~	83	~~84~~	~~85~~	~~86~~	~~87~~	~~88~~	89	~~90~~
~~91~~	~~92~~	~~93~~	~~94~~	~~95~~	~~96~~	97	~~98~~	~~99~~	~~100~~
101									

2.2 关于同余的一些基本定理

在这一节我想描述素性检验和求因子的一些古典方法. 它们依赖于同余式的一些定理、特别是费马小定理、古老的 Wilson 定理和欧拉对费马小定理的推广. 我还用一小节讲二次剩余, 这是非常重要的内容, 并且以后我会向大家表明, 它与素数检验也有联系.

2.2A 费马小定理和模 p原根

费马小定理 *若 p 为素数并且 a 为整数, 则 $a^p \equiv a \pmod{p}$. 特别若 a 不被 p 整除, 则 $a^{p-1} \equiv 1 \pmod{p}$.*

欧拉发表了费马小定理的第一个证明.

证明 当 $a = 1$ 时显然成立. 假设定理对 a 成立, 由归纳法知 $(a+1)^p \equiv a^p + 1 \equiv a + 1 \pmod{p}$. 所以定理对每个自然数 a 均正确. □

上面的证明只需要一个事实: 若 p 为素数而 $1 \leqslant k \leqslant p-1$, 则二项式系数 $\binom{p}{k}$ 都是 p 的倍数.

定理的直接推论是: 若 $p \nmid a$, 而 $p^n \| a^p - 1$(这表示 $p^n \mid a^p - 1$ 但是 $p^{n+1} \nmid a^p - 1$), 则对每个 $e \geqslant 1$, $p^{n+e} \| a^{p^e(p-1)} - 1$. 注意对于 $p = 2$, 则 n 至少为 2 ①.

由定理还可推出, 对每个不被 p 除尽的整数 a, 均存在最小的指数 $h \geqslant 1$, 使得 $a^h \equiv 1 \pmod{p}$. 进而, $a^k \equiv 1 \pmod{p}$ 当且仅当 $h \mid k$. 特别地, $h \mid p-1$. 这个指数 h 叫作 a 模 p 的阶. 注意 $a, a^2, \cdots, a^{h-1}$ 和 1 模 p 是彼此不同的.

① 实际上 n 至少为 3—— 译者注.

一个基本的事实是: 对每个素数 p, 均至少存在一个整数 $g(p \nmid g)$, 使得 g 模 p 的阶等于 $p-1$. 这时, 集合 $\{1, g, \cdots, g^{p-2}\}$ 在模 p 的意义下等于集合 $\{1, 2, \cdots, p-1\}$.

每个模 p 阶为 $p-1$ 的整数 $g(1 \leqslant g \leqslant p-1)$ 叫作模 p 的一个原根. 我们有如下的命题:

设 p 为奇素数, $k \geqslant 1, S = \sum_{j=1}^{p-1} k^j$. 则

$$S \equiv \begin{cases} -1 \pmod p, & p-1 \mid k \\ 0 \pmod p, & p-1 \nmid k \end{cases}$$

证明 如果 $p-1 \mid k$, 则对于 $1 \leqslant j \leqslant p-1$, $j^k \equiv 1 \pmod p$. 从而 $S \equiv p-1 \equiv -1 \pmod p$. 如果 $p-1 \nmid k$, 取模 p 的一个原根 g, 则 $g^k \not\equiv 1 \pmod p$. 由于在模 p 的意义下, 集合 $\{1, 2, \cdots, p-1\}$ 与 $\{g, 2g, \cdots, (p-1)g\}$ 相等. 所以

$$g^k S \equiv \sum_{j=1}^{p-1} (gj)^k \equiv \sum_{j=1}^{p-1} j^k \equiv S \pmod p$$

从而 $(g^k - 1)S \equiv 0 \pmod p$. 但是 $p \nmid g^k - 1$, 于是 $S \equiv 0 \pmod p$.

□

高斯在《算术探究》一书的 73 、74 节中给出求模 p 一个原根的一个简单有效的方法. 它的程序为:

第 1 步: 任取一个整数 a, $1 < a < p$(如取 $a = 2$). 写出 $a, a^2, a^3, \cdots$ 的模 p 剩余. 令 t 为最小正整数使得 $a^t \equiv 1 \pmod p$. 如果 $t = p-1$, 则 a 是模 p 的一个原根. 否则作下一步.

第 2 步: 取任一个整数 b, $1 < b < p$ 并且 $b \not\equiv a^i \pmod p$ $(1 \leqslant i \leqslant t)$. 令 u 是满足 $b^u \equiv 1 \pmod p$ 的最小正整数. 易知 $u \nmid t$, 否则 $b^t \equiv 1 \pmod p$, 但是 $1, a, a^2, \cdots, a^{t-1}$ 是同余方程

$X^t \equiv 1 \pmod p$ 的 t 个模 p 不同的解，从而也是这个同余方程的全部解. 于是 $b \equiv a^m \pmod p$(对某个 m, $0 \leqslant m \leqslant t-1$), 而这与假设矛盾. 如果 $u \neq p-1$, 记 v 为 t 和 u 的最小公倍数, 则 $v = mn$, 其中 $m \mid u, n \mid u$, 并且 $\gcd(m,n) = 1$. 令 $a' \equiv a^{t/m} \pmod p$, $b' \equiv b^{u/n} \pmod p$, 则 $c = a'b'$ 模 p 的阶为 $mn = v$. 如果 $v = p-1$, 则 c 是模 p 的一个原根. 否则再用类似于第 2 步的方式做下去.

由于 $v > t$, 所以每一步完成之后，或者给出模 p 的一个原根，或者得到一个整数，它的模 p 有更大的阶. 所以这个程序必定会停止于得到一个模 p 阶为 $p-1$ 的整数，这个整数就是模 p 的一个原根.

高斯用 $p = 73$ 来说明这个程序，发现 $g = 5$ 是模 73 的一个原根.

上面程序可给出模 p 的一个原根，但它不必是模 p 的最小原根 g_p $(1 < g_p < p)$. 为决定 g_p 需要依次决定 $a = 2, 3, \cdots$ 模 p 的阶. 不存在统一的方法, 对所有的素数 p 来预测模 p 最小原根. 但是关于 g_p 的大小有一些结果. 1944 年 Pillai 证明了：存在无穷多个素数 p, 使 $g_p > C \lg\lg p$(这里 C 是一个正的常数). 特别地, $\limsup_{p\to\infty} g_p = \infty$. 几年之后，利用关于算术级数中素数分布的 Linnik 深刻定理 (见第四章),Fridlender(1949) 和 Salié(1950) 独立地证明了对无穷多个 p, $g_p > C \lg p$, 其中 C 是某个正的常数. 另一方面， g_p 不能增长得太快， 1962 年 Burgess 证明了对充分大的 p

$$g_p \leqslant Cp^{1/4+\varepsilon} \quad (\varepsilon > 0, C > 0 \text{为常数})$$

Grosswald(1981) 将 Burgess 结果改进得更加明确: 若 $p > e^{e^{24}}$, 则 $g_p < p^{0.499}$②.

Vinogradov 证明的一个较弱的结果 (用 1/2 代替 1/4) 已收在

② 在这方面，中国解析数论学者们有不少更好得结果 —— 译者注.

Landau 的《数论讲义》(Vorlesungen über Zahlentheorie), 第 VII 部分，第十四章之中 (见本书“一般参考文献”).

下面是一个初等结果 (问题由 Powell 于 1983 年提出，而由 Kearnes 在 1984 年解决).

对每个正整数 M, 存在无穷多个素数 p, 使得 $M < g_p < p - M$.

下面的表 2.1 对于所有素数 $p < 1000$ 给出模 p 最小原根.

粗粗地看一下这个表格就会提出一个问题： 2 是否为无穷多个素数的原根？更一般地，若 $a \neq \pm 1$ 并且不是平方数， a 是否为无穷多个素数的原根？这是一个困难的问题，在第四章我要回到这个问题.

2.2B Wilson 定理

Wilson 定理 *若 p 为素数，则 $(p-1)! \equiv -1 \pmod{p}$.*

证明 这是费马小定理的一个推论. 因为 $1, 2, \cdots, p-1$ 是同余方程 $X^{p-1} - 1 \equiv 0 \pmod{p}$ 的根，而根的个数不能多于多项式次数，于是

$$X^{p-1} - 1 \equiv (X-1)(X-2)\cdots(X-(p-1)) \pmod{p}$$

比较常数项，得到 $-1 \equiv (-1)^{p-1}(p-1)! = (p-1)! \pmod{p}$(当 $p = 2$ 时此式也对). □

Wilson 定理给出素数的一种刻画方式. 设 $N > 1$ 为自然数，如果 N 不是素数，则 $N = mn (1 \leqslant m, n \leqslant N-1)$ 于是 m 为 N

和 $(N-1)!$ 的公因子，这表明 $(N-1)! \not\equiv -1 \pmod N$.

表 2.1　模 p 最小原根

p	g_p	p	g_p	p	g_p	p	g_p	p	g_p	p	g_p
2	1	127	3	283	3	467	2	661	2	877	2
3	2	131	2	293	2	479	13	673	5	881	3
5	2	137	3	307	5	487	3	677	2	883	2
7	3	139	2	311	17	491	2	683	5	887	5
11	2	149	2	313	10	499	7	691	3	907	2
13	2	151	6	317	2	503	5	701	2	911	17
17	3	157	5	331	3	509	2	709	2	919	7
19	2	163	2	337	10	521	3	719	11	929	3
23	5	167	5	347	2	523	2	727	5	937	5
29	2	173	2	349	2	541	2	733	6	941	2
31	3	179	2	353	3	547	2	739	3	947	2
37	2	181	2	359	7	557	2	743	5	953	3
41	6	191	19	367	6	563	2	751	3	967	5
43	3	193	5	373	2	569	3	757	2	971	6
47	5	197	2	379	2	571	3	761	6	977	3
53	2	199	3	383	5	577	5	769	11	983	5
59	2	211	2	389	2	587	2	773	2	991	6
61	2	223	3	397	5	593	3	787	2	997	7
67	2	227	2	401	3	599	7	797	2		
71	7	229	6	409	21	601	7	809	3		
73	5	233	3	419	2	607	3	811	3		
79	3	239	7	421	2	613	2	821	3		
83	2	241	7	431	7	617	3	823	3		
89	3	251	6	433	5	619	2	827	2		
97	5	257	3	439	15	631	3	829	2		
101	2	263	5	443	2	641	3	839	11		
103	5	269	2	449	3	643	11	853	2		
107	2	271	6	457	13	647	5	857	3		
109	6	277	5	461	2	653	2	859	2		
113	3	281	3	463	3	659	2	863	5		

但是，Wilson 这种对素数的刻画方式对于判定 N 的素性没有实际价值，因为目前没有好的算法来快速计算 $N!$(比如说，没

有 $\lg N$ 步的算法).

2.2C Giuga 和 Wolstenholme 性质

现在考虑素数的另一些性质. 首先, 若 p 为素数, 则由费马小定理有

$$1^{p-1}+2^{p-1}+\cdots+(p-1)^{p-1}\equiv -1\ (\mathrm{mod}\ p)$$

1950 年 Giuga 问反命题是否成立: 若 $n>1$ 并且 n 整除 $1^{n-1}+2^{n-1}+\cdots+(n-1)^{n-1}+1$, 则 n 是否必为素数?

容易证明, n 满足 Giuga 条件当且仅当对 n 的每个素因子 p, 均有 $p^2(p-1)\mid n-p$. 因为记 $n=pt$, 则 Giuga 条件变成

$$A=1+\sum_{j=1}^{pt-1}j^{pt-1}\equiv 0\ (\mathrm{mod}\ p)$$

而条件 $p^2(p-1)\mid pt-p$ 等价于 p 和 $p-1$ 均整除 $t-1$. 但是 $pt-1=(p-1)t+(t-1)$, 由费马小定理

$$A\equiv 1+\sum_{j=1}^{pt-1}j^{t-1}\equiv 1+tS\ (\mathrm{mod}\ p)$$

其中 $S=\sum\limits_{j=1}^{p-1}j^{t-1}$. 因此

$$A\equiv\begin{cases}1-t\ (\mathrm{mod}\ p), & p-1\mid t-1\\ 1\ (\mathrm{mod}\ p), & p-1\nmid t-1\end{cases}$$

所以当 $A\equiv 0\ (\mathrm{mod}\ p)$ 时, $p-1$ 和 p 均整除 $t-1$. 反过来, 这后两个条件推出 $A\equiv 0\ (\mathrm{mod}\ p)$ 并且 $p\nmid t$, 从而 n 无平方因子, 因此 $A\equiv 0\ (\mathrm{mod}\ n)$. □

由此可知，若 n 满足 Giuga 条件，则对 n 的每个素因子 $p,n \equiv p \equiv 1 \pmod{p-1}$. 这表明当 $p \mid n$ 时必有 $p-1 \mid n-1$. 满足这个条件的合成数叫作 Carmichael 数.

我在 2.9 节将指出这个条件是很强的限制. 但不管怎样，现在已经知道，若合成数 n 满足 Giuga 条件，则 n 至少有 12000 位，见 Bedocchi(1985),Borwein 和 Girgensohn(1996).

Wolstenholme 性质

1862 年，Wolstenholme 证明了如下一个有趣的结果：若 $p \geqslant 5$ 为素数，则

$$1+\frac{1}{2}+\frac{1}{3}+\cdots+\frac{1}{p-1}$$

的分子被 p^2 整除，而

$$1+\frac{1}{2^2}+\frac{1}{3^2}+\cdots+\frac{1}{(p-1)^2}$$

的分子被 p 整除.

证明可见 Hardy 和 Wright(1938) 的书 (见本书的一般参考文献). 根据这个性质不难推出，若 $n \geqslant 5$ 为素数，则

$$\binom{2n-1}{n-1} \equiv 1 \pmod{n^3}$$

反过来是否成立？这个问题是由 J.P.Jones 在许多年以前提出的，至今未能解决. 如果答案是肯定的，将会对素数给出形式简单的一个有趣的刻画.

这个问题自然地引出下面一些概念和问题. 设 $n \geqslant 5$ 为奇数，记

$$A(n)=\binom{2n-1}{n-1}$$

对每个 $k \geqslant 1$ 可以考虑集合

$$W_k = \{\text{奇数 } n \geqslant 5 \mid A(n) \equiv 1 \pmod{n^k}\}$$

则 $W_1 \supset W_2 \supset W_3 \supset W_4 \supset \cdots$. 由 Wolstenholme 定理可知，每个大于 3 的素数均属于 W_3.Jones 的问题相当于：W_3 是否恰好是大于 3 的全部素数组成的集合？

属于 W_4 的素数叫作 Wolstenholme 素数. 今天只知道两个 Wolstenholme 素数：Selfridge 和 Pollack 于 1964 年发现的 16843 和 Carndall,Ernvall,Metsänkylä 于 1993 年发现的 2124679. McIntosh 在 1995 年通过计算得到，在 $p < 5\times10^8$ 时没有新的 Wolstenholme 素数.

W_2 中包含所有 Wolstenholme 素数的平方. McIntosh 猜想它们是 W_2 中的全部合成数，并且验证了这个猜想在 10^9 以内是对的： W_2 中 10^9 以内的合成数只有 $n = 283686649 = 16843^2$.

McIntosh 认为存在无穷多个 Wolstenholme 素数. 要证这个论断是很困难的.

2.2D 素数整除 $a!$ 的最大方幂

1808 年，勒让德决定了素数 p 整除 $a!$ 的最大方幂 (即 $p^m \| a!$ 的 m). 将 a 表示 p 进制形式

$$a = a_k p^k + a_{k-1}p^{k-1} + \cdots + a_1 p + a_0$$

其中 $p^k \leqslant a < p^{k+1}$ 而 $0 \leqslant a_i \leqslant p-1 (i = 0,1,\cdots,k)$. 整数 $a_0, a_1, \cdots, a_k$ 叫作 a 的 p 进展开中的各位数字.

例如，对于 5 进展开， $328 = 2\cdot5^3 + 3\cdot5^2 + 3$, 从而 328 的 5 进展开式中各位数字为 2, 3, 0, 3. 采用这种记号，我们有

勒让德定理

$$m = \sum_{i=1}^{\infty} \left[\frac{a}{p_i}\right] = \frac{a - (a_0 + a_1 + \cdots + a_k)}{p - 1}$$

证明 根据定义，$a! = p^m b$, $p \nmid b$. 记 $a = q_1 p + r_1, q_1 \geqslant 0$, $0 \leqslant r_1 < p$. 则 $q_1 = [\frac{a}{p}]$. 不超过 a 的整数中被 p 整除的为 $p, 2p, \cdots, q_1 p\ (\leqslant a)$. 于是 $p^{q_1}(q_1!) = p^m b'$, $p \nmid b'$. 这表明 $q_1 + m_1 = m$, 其中 $p^{m_1} \| q_1!$. 由于 $q_1 < a$, 可用归纳法得到

$$m_1 = \left[\frac{q_1}{p}\right] + \left[\frac{q_1}{p^2}\right] + \left[\frac{q_1}{p^3}\right] + \cdots$$

但是容易验证

$$\left[\frac{q_1}{p^i}\right] = \left[\frac{[a/p]}{p^i}\right] = \left[\frac{a}{p^{i+1}}\right]$$

从而

$$m = \left[\frac{a}{p}\right] + \left[\frac{a}{p^2}\right] + \left[\frac{a}{p^3}\right] + \cdots$$

现在对于 p 进展开 $a = a_k p^k + \cdots + a_1 p + a_0$, 得到

$$\begin{aligned}
\left[\frac{a}{p}\right] &= a_k p^{k-1} + \cdots + a_1 \\
\left[\frac{a}{p^2}\right] &= a_k p^{k-2} + \cdots + a_2 \\
&\vdots \\
\left[\frac{a}{p^k}\right] &= a_k
\end{aligned}$$

于是

$$\sum_{i=0}^{\infty}\left[\frac{a}{p^i}\right]=a_1+a_2(p+1)+a_3(p^2+p+1)+\cdots$$

$$+a_k(p^{k-1}+p^{k-2}+\cdots+p+1)$$

$$=\frac{1}{p-1}\{a_1(p-1)+a_2(p^2-1)+\cdots+a_k(p^k-1)\}$$

$$=\frac{1}{p-1}\{a-(a_0+a_1+\cdots+a_k)\}$$ □

1852 年，Kummer 用勒让德的结果决定了 $p^m\|\binom{a+b}{a}$ 的 m, 其中

$$\binom{a+b}{a}=\frac{(a+b)!}{a!b!}\qquad(a\geqslant 1,b\geqslant 1)$$

令

$$a=a_0+a_1p+\cdots+a_tp^t$$

$$b=b_0+b_1p+\cdots+b_tp^t$$

其中 $0\leqslant a_i,b_i\leqslant p-1$, 并且 a_t 和 b_t 至少有一个不为零. 记 $S_a=\sum\limits_{i=0}^{t}a_i$ 和 $S_b=\sum\limits_{i=0}^{t}b_i$ 分别为 p 进展开式的数字和. 如下依次定义 c_i $(0<c_i\leqslant p-1)$ 和 $\varepsilon_i\in\{0,1\}$:

$$a_0+b_0=\varepsilon_0p+c_0$$

$$\varepsilon_0+a_1+b_1=\varepsilon_1p+c_1$$

$$\vdots$$

$$\varepsilon_{t-1}+a_t+b_t=\varepsilon_tp+c_t$$

将这些等式分别乘以 $1, p, p^2, \cdots$ 然后相加，得到

$$
\begin{aligned}
& a+b+\varepsilon_0 p+\varepsilon_1 p^2+\cdots+\varepsilon_{t-1} p^t \\
= & \varepsilon_0 p+\varepsilon_1 p^2+\cdots+\varepsilon_{t-1} p^t+\varepsilon_t p^{t+1}+c_0+c_1 p+\cdots+c_t p^t
\end{aligned}
$$

因此 $a+b=c_0+c_1p+\cdots+c_tp^t+\varepsilon_tp^{t+1}$，这是 $a+b$ 的 p 进展开式. 类似地，将这些等式相加，得到

$$S_a+S_b+(\varepsilon_0+\varepsilon_1+\cdots+\varepsilon_{t-1})=(\varepsilon_0+\varepsilon_1+\cdots+\varepsilon_t)p+S_{a+b}-\varepsilon_t$$

由勒让德结果

$$
\begin{aligned}
(p-1)m &= (a+b)-S_{a+b}-a+S_a-b+S_b \\
&= (p-1)(\varepsilon_0+\varepsilon_1+\cdots+\varepsilon_t)
\end{aligned}
$$

从而证明了如下结果:

Kummer 定理 *若 $p^m \| \binom{a+b}{a}$，则 $m=\varepsilon_0+\varepsilon_1+\cdots+\varepsilon_t$，它们是将 a 和 b 按 p 进制相加时进位的次数.*

Lucas 于 1878 年又重新发现了 Kummer 的这个定理. 1991 年， Frasney 把这个结果进一步推广到 p 进整数的情形.

勒让德和 Kummer 的结果在 p 进分析中有许多应用，在本书第三章 3.3 节也有应用.

2.2E 中国剩余定理

我的兴趣虽然主要在素数，但是无法避免研究一般整数的问题，特别是在许多问题中要同时考虑多个素数的时候，因为整数以唯一的方式分解成素数方幂的乘积.

整数 n 及其素数幂因子之间的一个关键性的联系是很古老的，熟知它来源于古代中国，所以叫作中国剩余定理. 但是 A.

Zachariou 在私人通信中告诉我，在这之前希腊人就知道这个结果．由于希腊人发现了许多定理，我对这个结果还是采用传统的名称．我相信每个读者都知道它：

若 $n_1, n_2, \cdots, n_k$ 是大于 1 的两两互素的整数，而 $a_1, a_2, \cdots, a_n$ 为任何整数，则存在整数 a，使得

$$\begin{cases} a \equiv a_1 \pmod{n_1} \\ a \equiv a_2 \pmod{n_2} \\ \quad\vdots \\ a \equiv a_k \pmod{n_k} \end{cases}$$

进而，整数 a' 也满足上述同余式组当且仅当 $a \equiv a' \pmod{n_1 n_2 \cdots n_k}$．所以在 $0 \leqslant a < n_1 n_2 \cdots n_k$ 条件下有唯一的整数 a 满足上述同余式组．

证明很简单，可在许多书中找到，也可见 Mozzochi(1967) 的短文．

中国剩余定理有许多应用．据说这是中国将军们清点士兵人数的方法：

七七报数！

七人一行排队！

十一人一行排队！

十三人一行排队！

十七人一行排队！

每次只计算不够一行的人数，聪明的将军可以知道士兵确切

的人数[3].

下面是中国剩余定理的另一个应用. 若 $n = p_1 p_2 \cdots p_k$ 是不同素数的乘积. 如果 g_i 为模 p 的原根 $(1 \leqslant i \leqslant k)$, 而 g 为整数, $1 \leqslant g \leqslant n-1$, 并且对每个 $i = 1, 2, \cdots, k$, $g \equiv g_i \pmod{p_i}$, 则 g 模 p_i 的阶为 $p_i - 1$ $(1 \leqslant i \leqslant k)$, 并且 g 模 n 的阶为 $\prod_{i=1}^{k}(p_i - 1)$[4].

2.2F 欧拉函数

欧拉引入一个函数 (欧拉函数), 用以推广费马小定理.

对每个 $n \geqslant 1$, 以 $\varphi(n)$ 表示从 1 到 n 之中与 n 互素的整数个数. 如果 $n = p$ 为素数, 则 $\varphi(p) = p - 1$. 进一步

$$\varphi(p^k) = p^{k-1}(p-1) = p^k\left(1 - \frac{1}{p}\right)$$

又若 m 和 n 是互素的正整数, 则 $\varphi(mn) = \varphi(m)\varphi(n)$, 即 φ 是积性函数. 于是对每个整数 $n = \prod_p p^k$(乘积过 n 的所有素因子, $k \geqslant 1$), 则

$$\varphi(n) = \prod_p p^k(p-1) = n\prod_p\left(1 - \frac{1}{p}\right)$$

另一个简单性质为: $n = \sum_{d|n} \varphi(d)$.

欧拉证明了欧拉定理:

欧拉定理 若 $\gcd(a, n) = 1$, 则 $a^{\varphi(n)} \equiv 1 \pmod{n}$.

证明 记 $r = \varphi(n)$. 令 $b_1, \cdots, b_r$ 是模 n 彼此不同余并且均与 n 互素的整数, 则 $ab_1, \cdots, ab_r$ 仍具有这些性质. 于是集合

---

③ 关于中国剩余定理的确切历史, 可见中国数论书籍 (如华罗庚《数论导引》) 所述 —— 中译者.

④ 应当为 $p_i - 1$ $(1 \leqslant i \leqslant k)$ 的最小公倍数 —— 中译者.

$\{b_1, \cdots, b_r\}$ 和 $\{ab_1, \cdots, ab_r\}$ 模 p 为同样的集合. 从而

$$a^r \prod_{i=1}^{r} b_i = \prod_{i=1}^{r} ab_i \equiv \prod_{i=1}^{r} b_i \pmod n$$

这表明

$$(a^r - 1) \prod_{i=1}^{r} b_i \equiv 0 \pmod n$$

因此 $a^r \equiv 1 \pmod n$. □

像讲述费马小定理时的情形一样, 由欧拉定理也可得出, 存在最小正整数 e 使得 $a^e \equiv 1 \pmod n$.e 叫作 a 模 n 的阶. 若 n 为素数, 这个定义与前面一致. 我们也有: $a^m \equiv 1 \pmod n$ 当且仅当 $e|m$. 特别地, $e|\varphi(n)$.

人们自然要问: 给了 $n > 2$, 是否一定存在与 n 互素的整数 a, 使得 a 模 n 的阶为 $\varphi(n)$? 回忆当 $n = p$ 为素数时, 这样的 a 是存在的, 即是模 p 的原根. 若 $n = p^e$(奇素数的方幂), 这也成立. 更精确地说, 下列三个命题是彼此等价的.

(i) g 为模 p 原根并且 $g^{p-1} \not\equiv 1 \pmod{p^2}$;

(ii) g 为模 p^2 原根;

(iii) 对每个 $e \geqslant 2$,g 是模 p^e 原根.

例如, 10 是模 487 的原根, 但是 $10^{486} \equiv 1 \pmod{487^2}$, 所以 10 不是模 487^2 的原根. 当 10 固定时这是说明这种现象的最小的例子. 另一个例子为 14 模 29.

但是当 n 被 $4p$ 或 pq 整除时 (其中 p 和 q 是不同的奇素数), 则没有与 n 互素的 a, 使得 a 模 n 的阶为 $\varphi(n)$. 这是由于: 不难看出 a 模 n 的阶最多为函数 $\lambda(n)$, 它是 Carmichael 于 1912 年按

下面方式定义的：

$$\lambda(1)=1,\ \lambda(2)=1,\ \lambda(4)=2$$

$$\lambda(2^r)=2^{r-2}\quad(r\geqslant 3)$$

$$\lambda(p^r)=p^{r-1}(p-1)=\varphi(p^r)\qquad(\text{对于每个奇素数 } p \text{ 和 } r\geqslant 1)$$

$$\lambda(2^r p_1^{r_1} p_2^{r_2}\cdots p_s^{r_s})=\operatorname{lcm}\{\lambda(2^r),\lambda(p_1^{r_1}),\cdots,\lambda(p_s^{r_s})\}$$

(这里 lcm 表示最小公倍数)

注意 $\lambda(n)$ 整除 $\varphi(n)$, 但可能比 $\varphi(n)$ 要小，而且有与 n 互素的整数 a, 使得 a 模 n 的阶为 $\lambda(n)$.

我想利用这个机会更仔细地讨论一下欧拉函数. 首先考虑 Lehmer 问题，然后研究 φ 的取值问题，包括取值重复度，不取哪些值，以及 φ 的平均值等.

Lehmer 问题

对于素数 p,$\varphi(p)=p-1$.Lehmer 在 1932 年问：是否存在合成数 n, 使得 $\varphi(n)\mid n-1$ ？这个问题至今没有解决，而且在今天看来，离解决此问题似乎仍旧和 Lehmer 在 70 年前提出它时一样的遥远. 如果答案是否定的，将给出素数的又一个刻画.

如果不能解决这个问题，我们还可以说些什么？有许多原因显示出不大可能有合成数 n, 使得 $\varphi(n)|n-1$.

(a) 这种数一定很大 (如果存在的话)；

(b) 这种数一定有许多素因子 (如果存在的话)；

(c) 不超过 x 的这种数的个数有上界 $f(x)$, 其中 $f(x)$ 与 x 相比是很小的函数.

Lehmer 在 1932 年证明了：若 n 是合成数并且 $\varphi(n)|n-1$, 则 n 为无平方因子的奇数, 并且它的不同素因子个数 $\omega(n)\geqslant 7$. 后来 Schuh(1944) 又改进为 $\omega(n)\geqslant 11$.1970 年， Lieuwens 证明了：若

$3|n$, 则 $\omega(n) \geqslant 213$ 并且 $n > 5.5 \times 10^{570}$. 而当 $30 \nmid n$ 时, $\omega(n) \geqslant 13$.

记录

1980 年 Cohen 和 Hagis 证明了: 若 n 为合成数并且 $\varphi(n)|n-1$, 则 $n > 10^{20}$ 并且 $\omega(n) \geqslant 14$.Wall(1980) 证明了: 若 $\gcd(30, n) = 1$, 则 $\omega(n) \geqslant 26$. 而当 $3|n$ 时, Lieuwens 的结果目前仍是最好的.

1977 年 Pomerance 证明了: 对每个充分大的正实数 x, 以 $L(x)$ 表示满足 $\varphi(n)|n-1$ 和 $n \leqslant x$ 的合成数个数, 则

$$L(x) \leqslant x^{1/2}(\lg x)^{3/4}$$

并且当 $\omega(n) = k$ 时, $n < k^{2^k}$.

欧拉函数的取值

不难证明: 欧拉函数值不能取遍所有正偶数. 比如 Schinzel 在 1956 年证明了, 对每个 $k \geqslant 1$, 2×7^k 都不是欧拉函数值.

1976 年 Mendelsohn 证明了: 存在无穷多个素数 p, 使得对每个 $k \geqslant 1$,$2^k p$ 均不是欧拉函数值. 关于欧拉函数有趣的取值, Erdös 于 1946 年提出一个猜想: 对每个 $k \geqslant 1$ 均有 n 使得 $\varphi(n) = k!$.Lambak 于 1948 年给出此问题的解, 后来又由 Gupta(1950) 给出同样结果.

下面结果表明欧拉函数值的分布是多么混乱. Somayajulu 于 1950 年证明了

$$\limsup_{n\to\infty} \frac{\varphi(n+1)}{\varphi(n)} = \infty, \qquad \liminf_{n\to\infty} \frac{\varphi(n+1)}{\varphi(n)} = 0$$

这个结果由 Schinzel 和 Sierpiński 加以改进, 见 Schinzel(1954): 所有 $\varphi(n+1)/\varphi(n)$ 组成的集合在正实数集合中稠密.

Schinzel,Sierpiński(1954) 和 Schinzel(1954) 中还证明了: 对每

个 $m,k\geqslant 1$, 存在 $n,h\geqslant 1$ 使得对所有 $i=1,2,\cdots,k$ 均有

$$\frac{\varphi(n+i)}{\varphi(n+i-1)}>m,\qquad \frac{\varphi(h+i-1)}{\varphi(h+i)}>m$$

最后，所有 $\varphi(n)/n$ 组成的集合在区间 $(0,1)$ 中稠密.

欧拉函数值的重复度

现在谈欧拉函数的“重复度”，即考察一个函数值 $\varphi(n)$ 可以取多少次. 为了系统地解释这方面的结果，最好引入某些记号. 对于 $m\geqslant 1$, 令

$$V_\varphi(m)=\#\{n\geqslant 1\mid\varphi(n)=m\}$$

$V_\varphi(m)$ 都可能取哪些值？我已经说过：存在无穷多个偶数 m, 使得 $V_\varphi(m)=0$. 下面事情也是对的：对于 $m=2\times 3^{6k+1}$ $(k\geqslant 1)$, 则 $\varphi(n)=m$ 恰好在 $n=3^{6k+2}$ 或者 $n=2\times 3^{6k+2}$ 的时候. 所以有无穷多整数 m, 使得 $V_\varphi(m)=2$.

不难证明对每个 $m\geqslant 1$, $V_\varphi(m)\neq\infty$.

Pillai(1929) 有以下结果：

$$\sup\{V_\varphi(m)\}=\infty$$

Schinzel 于 1956 年给出一个简单的证明. 换句话说，对每个 $k\geqslant 1$, 均有整数 m_k, 使得存在至少 k 个整数 n, 使得 $\varphi(n)=m_k$.

Sierpiński 有一个更强的猜想: 对每个整数 $k\geqslant 2$, 均存在 $m>1$, 使得 $k=V_\varphi(m)$. 采用很精细的方法， Ford(1999) 证明了这个猜想.

Carmichael 猜想

在欧拉函数取值重复度方面起主导作用的是 Carmichael 于 1922 年提出的以下猜想： 1 不是 V_φ 的取值. 也就是说，给了任何 $n\geqslant 1$ 均有 $n'\geqslant 1$, $n'\neq n$, 使得 $\varphi(n')=\varphi(n)$.

1947 年， Klee 证明了此猜想对 $\varphi(n) < 10^{400}$ 的每个 n 成立. 利用 Klee 的方法， Masai 和 Valette (1982) 改进到 $\varphi(n) < 10^{10000}$.Schlafly 和 Wagon 本质上仍采用 Klee 方法但加入大量计算，于 1994 年将此猜想反例的下界提高很多：如果 $V_\varphi(n) = 1$, 则 $n > 10^{10^7}$.Ford(1998) 采用更有力的方法，进一步将此下界改进为 $n > 10^{10^{10}}$.

Wagon 对 Carmichael 猜想也写过一篇文章, 登在 *The Mathematical Intelligencer* (1986) 上. 计算结果均支持 Carmichael 猜想是对的. 但是 Pomerance(1974) 证明了：如果 $m \geqslant 1$, 并且对每个满足条件 $p-1 \mid \varphi(m)$ 的素数 p 均有 $p^2 \mid m$, 则 $V_\varphi(\varphi(m)) = 1$.

于是，若满足上述条件的 m 存在，则 Carmichael 猜想不正确. 但是这种 m 的存在性问题一直未能解决, 很可能是不存在的.

关于 Carmichael 猜想近来最重要的结果是 K.Ford(1998) 给出的. 对每个 $x > 0$, 令 $E(x) = \#\{n \mid 1 \leqslant n < x, \text{并且存在} k > 1, \text{使 } \varphi(k) = n\}$, $E_1(x) = \#\{n \mid 1 \leqslant n \leqslant x, \text{并且存在唯一的} k, \text{使 } \varphi(k) = n\}$.Carmichael 猜想是说对每个 $x > 0, E_1(x) = 0$. 而 Ford 证明了：若 Carmichael 猜想不成立，则存在 $C > 0$, 使得对充分大的 x, 均有 $E(x) \leqslant CE_1(x)$. 由此提出 Carmichael 猜想等价于

$$\liminf_{x \to \infty} \frac{E_1(x)}{E(x)} = 0$$

Ford 还证明了 $E_1(10^{10^{10}}) = 0$.

最后，作为 Carmichael 猜想的一个推广，人们相信每个 $s > 1$ 都是 V_φ 的取值，这是 Sierpiński 的一个猜想. 我在第六章 6.2 节要指出，这是另一个未被证明的有趣猜想的推论.

V_φ 的取值重复度又会怎样呢？我已经提到过，存在无穷多个 m 不是 φ 的取值，即 $V_\varphi(m) = 0$. 所以 V_φ 无穷多次取值为 0. Erdös 在 1958 年将此作了推广：若 $s \geqslant 1$ 为 V_φ 的取值，则 V_φ 必

然无穷多次取值为 s(请用欧拉函数的语言直接叙述这个结果，以检验你是否理解我的数学记号).

欧拉函数的增长程度

我还没有谈及函数 φ 的增长程度. 由 $\varphi(p)=p-1$(对每个素数 p) 可知 $\limsup(\varphi(n))=\infty$. 类似可知 $\limsup\varphi(n)/n=1$. 关于 φ 的增长性状的其他结果将在第四章中介绍，因为要用到第四章中所讨论的方法.

2.2G 二项式序列

前面的讨论涉及到模一个给定的整数 $n>1$ 的同余式，而 a 是与 n 互素的任何正整数. 另一种观点也是有趣的，即给定 $a>1$，而考虑整数序列 a^n-1 $(n\geqslant 1)$ 和它的伴随序列 a^n+1 $(n\geqslant 1)$. 更一般地，对于 $a>b\geqslant 1$, $\gcd(a,b)=1$, 考虑序列 a^n-b^n $(n\geqslant 1)$ 和 a^n+b^n $(n\geqslant 1)$.

第一个自然的问题是：决定所有的素数 p, 使得存在 $n\geqslant 1$, 使得 $p\mid a^n-b^n$. 这个问题答案很简单：就是 $p\nmid ab$ 的那些素数 p. 必然性是由于 a 和 b 互素. 而若 $p\nmid ab$, 则 $bb'\equiv 1 \pmod p$. 令 n 为 ab' 模 p 的阶，则 $p\mid a^n-b^n$.

二项式 a^n+b^n 要复杂些. 若 $p\neq 2$, 并且存在 $n\geqslant 1$ 使得 $p\mid a^n+b^n$, 则 $p\nmid ab(a-b)$. 但反命题不成立. 例如，对每个 $n\geqslant 1$, $7\nmid 2^n+1$.

本原素因子

如果 $n\geqslant 1$ 是满足 $p\mid a^n-b^n$(或 $p\mid a^n+b^n$) 的最小整数，称 p 是 a^n-b^n(或 a^n+b^n) 的本原素因子. 这时，由费马小定理可知 $n\mid p-1$. 勒让德就已经明确地指出这个结论. 所以每个素数

$p \nmid ab$ 都是某个二项式 $a^n - b^n$ 的本原因子. 反过来, 是否每个二项式都有本原因子?

Zsigmondy 于 1892 年证明了下面的有趣定理, 它有许多应用.

如果 $a > b \geqslant 1$ 并且 $\gcd(a, b) = 1$, 则除了 $a - b = 1, n = 1$; $2^6 - 1 = 63$ 和 $a^2 - b^2$ ($2 \nmid ab$ 并且 $a + b$ 是 2 的方幂) 之外, 每个数 $a^n - b^n$ 都有本原素因子.

类似地, 如果 $a > b \geqslant 1$, 则除了 $2^3 + 1 = 9$ 之外, 每个数 $a^n + b^n$ 都有本原素因子.

1886 年 Bang 证明了 $b = 1$ 的特殊情形. 后来又有许多数学家一再地 (有时是彼此不了解地) 证明这个定理或者是 Bang 结果的特殊情形. 他们是 Birkhoff 和 Vandiver (1904), Carmichael (1913), Kanold (1950), Artin (1955), Lüneburg(1981). 可能还有其他人.

证明肯定不是显然的, 但是很容易写下这些序列, 然后观察依次出现新的本原素因子.

另一个有趣的事情是考虑 $a^n - b^n$ 的本原部分 t_n^*, 即 $a^n - b^n = t_n^* t_n'$, $\gcd(t_n^*, t_n') = 1$, 并且 $p \mid t_n^*$ 当且仅当 p 是 $a^n - b^n$ 的本原素因子.

通过对序列 $a^n - b^n$ 的数据试验, 发现除了开始几项之外, t_n^* 都是合成数. 事实上, Schinzel 在 1962 年证明了以下定理:

令 $k(m)$ 为 m 的无平方因子部分, 即 m 除去它的最大平方因子. 又令

$$e = \begin{cases} 1, & k(ab) \equiv 1 \pmod 4 \\ 2, & k(ab) \equiv 2, 3 \pmod 4 \end{cases}$$

设 $n/ek(ab)$ 为奇整数并且 $n>1$, 则除了少数个例外 (最大可能的例外是 $n=20$)a^n-b^n 至少有两个不同的本原素因子. 当 $n>1$ 和 $b=1$ 时, 例外为

$$若\ a=2:\ n=4,12,20$$

$$若\ a=3:\ n=6$$

$$若\ a=4:\ n=3$$

从而有无穷多个 n, 使得 a^n-b^n 的本原部分是合成数.

Schinzel 还证明了: 如果 $ab=c^h$, 其中 $h\geqslant 3$, 或者 $h=2$, 同时 $k(c)$ 为奇数, 则有无穷多个 n, 使得 a^n-b^n 的本原部分至少有三个素因子.

对于序列 a^n+b^n, 易知若 $n/ek(ab)$ 为奇数并且 $n>10$, 则 a^n+b^n 的本原部分是合成数. 这是由于 $a^{2n}-b^{2n}$ 的本原素因子均为 a^n+b^n 的本原素因子.

下面一些问题都是很困难的:

是否有无穷多个 n, 使得 a^n-b^n 的本原部分为素数?

是否有无穷多个 n, 使得 a^n-b^n 的本原部分是无平方因子整数?

下面的问题也许容易一些:

是否有无穷多个 n, 使得 a^n-b^n 的本原部分 t_n^* 有素因子 p, 并且 $p^2\nmid a^n-b^n$?

是否有无穷多个 n, 使得 t_n^* 的无平方因子部分 $k(t_n^*)$ 大于 1 ?

这些问题甚至对于 $b=1$ 的特殊情形都与费马大定理有奇妙的联系!

最大素因子

另一个有趣的问题是估计 a^n-b^n 最大素因子的大小, 其

中 $a > b \geqslant 1$, $\gcd(a,b)=1$. 我们用 $P[m]$ 表示 $m \geqslant 1$ 的最大素因子.

用 Zsigmondy 定理不难证明, 当 $n > 2$ 时, $P[a^n - b^n] \geqslant n+1$.

1962 年, Schinzel 证明了对于 $n > 2$, 在下列情形有 $P[a^n - b^n] \geqslant 2n+1$： $4 \nmid n$(去掉情形 $a=2, b=1, n=6$)； $k(ab) \mid n$ 或 $k(ab)=2$(去掉情形 $a=2, b=1, n=4,6$ 或 12).

Erdös 在 1965 年猜想 $\lim_{n\to\infty} P[2^n-1]/n = \infty$. 尽管这方面有很好的工作, 这个猜想至今未完全解决. 但是有很好的部分结果, 我下面报告这些结果.

利用 Baker 关于对数线性型的不等式, Stewart 于 1975 年证明了：若 $0 < r < 1/\lg 2$, 以 S_r 表示具有最多 $r \lg\lg n$ 个不同素因子的整数 n 构成的集合 (集合 S_r 的密度为 1), 则

$$\lim_{\substack{n\to\infty \\ n\in S_r}} \frac{P[a^n-b^n]}{n} = \infty$$

这个表达式增长有多快？ Stewart 在 1977 年给出一个答案. 用更精确的 Baker 型不等式给出

$$\frac{P[a^n-b^n]}{n} > C\frac{(\lg n)^\lambda}{\lg\lg\lg n}$$

其中 $\lambda = 1 - r\lg 2, C > 0$ 是常数, 而 $n \in S_r$.Stewart 还证明了：对每个充分大的素数 $p, P[a^n-b^n]/p > C\lg p$ $(C>0)$. 对于 Mersenne 素数 2^p-1 这一特别情形, Erdös 和 Shorey 在 1976 年给出这个结果.

在数 a^n-1, 分圆多项式的值和某些算术级数中的素数之间有密切的联系, 但是我不能同时解释所有的事情, 请不要着急, 允许我在第四章 4.4 节再考虑这些事情.

2.2H 二次剩余

费马、欧拉、勒让德和高斯在研究二次不定方程的过程中，一个非常重要的事情是决定一个整数 a 何时为模一个奇素数 p 的平方．若奇素数 p 不整除 a, 如果存在整数 b 使得 $a \equiv b^2 \pmod{p}$,a 叫作模 p 的二次剩余，否则 a 叫作模 p 的非二次剩余．勒让德引入一个实用的符号

$$\left(\frac{a}{p}\right) = (a \mid p) = \begin{cases} +1, & a \text{ 为模 } p \text{ 的二次剩余} \\ -1, & \text{否则} \end{cases}$$

当 $p \mid a$ 时，通常定义 $(a \mid p) = 0$.

现在指出勒让德符号一些重要性质．这些性质也见于任何一本初等数论书.

若 $a \equiv a' \pmod{p}$, 则

$$\left(\frac{a}{p}\right) = \left(\frac{a'}{p}\right)$$

对任何整数

$$\left(\frac{aa'}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{a'}{p}\right)$$

为了计算勒让德符号，只需计算 $(q \mid p)$, 其中 $q = -1, 2$ 和与 p 不同的所有奇素数．欧拉证明了

$$\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p}$$

特别地

$$\left(\frac{-1}{p}\right) = \begin{cases} +1, & p \equiv 1 \pmod{4} \\ -1, & p \equiv -1 \pmod{4} \end{cases}$$

和

$$\left(\frac{2}{p}\right) = \begin{cases} +1, & p \equiv \pm 1 \pmod{8} \\ -1, & p \equiv \pm 1 \pmod{8} \end{cases}$$

再加上高斯的二次互反律：对于两个不同的奇素数 p 和 q

$$\left(\frac{p}{q}\right)=\left(\frac{q}{p}\right)(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$$

便可用一个容易的快速算法计算勒让德符号 $(q \mid p)$.

勒让德符号的重要性促使雅可比 (Jacobi) 考虑它的一个推广，现在叫作雅可比符号. 它也可参见许多文献，如 Grosswald 的书 (1966, 1984 年第二版), 或者作者的书 (1972,2001 年新增版).

设 a 为非零整数， b 为奇整数并且 $\gcd(a,b)=1$. 雅可比符号 $(a \mid b)$ 是勒让德符号的推广，它定义为：令 $b=\prod_{p\mid b} p^{e_p}>0$ $(e_p \geqslant 1)$, 则

$$\left(\frac{a}{b}\right)=\prod_{p\mid b}\left(\frac{a}{p}\right)^{e_p}$$

$$\left(\frac{a}{-b}\right)=\begin{cases}\left(\dfrac{a}{b}\right), & a>0\\ -\left(\dfrac{a}{b}\right), & a<0\end{cases}$$

所以 $(a \mid b)=\pm 1$. 注意

$$\left(\frac{a}{1}\right)=\left(\frac{a}{-1}\right)=+1 \quad (a>0)$$

下面是雅可比符号的一些性质：在定义中的假设之下

$$\left(\frac{aa'}{b}\right)=\left(\frac{a}{b}\right)\left(\frac{a'}{b}\right)$$

$$\left(\frac{a}{bb'}\right)=\left(\frac{a}{b}\right)\left(\frac{a}{b'}\right)$$

$$\left(\frac{-1}{b}\right)=(-1)^{(b-1)/2}=\begin{cases}+1, & b\equiv 1 \pmod 4\\ -1, & b\equiv -1 \pmod 4\end{cases}$$

$$\left(\frac{2}{b}\right)=(-1)^{(b^2-1)/8}=\begin{cases}+1, & b\equiv \pm 1 \pmod 8\\ -1, & b\equiv \pm 3 \pmod 8\end{cases}$$

在计算雅可比符号时，最关键结果是下面的互反律，它可由关于勒让德符号的高斯互反律直接推出来

$$\left(\frac{a}{b}\right)=\varepsilon\left(\frac{b}{a}\right)(-1)^{\frac{a-1}{2}\cdot\frac{b-1}{2}}$$

其中

$$\varepsilon=\begin{cases}+1, & a>0 \text{ 或者 } b>0\\ -1, & a<0 \text{ 并且 } b<0\end{cases}$$

最后若 $b\geqslant 3$ 并且 a 是模 b 的平方，则 $(a\mid b)=+1$.

2.3 基于同余式的经典素性判定方法

在介绍了费马、Wilson 和欧拉定理之后，我现在介绍基于同余式的一些经典的素性判定方法，这指的是 Lehmer 扩充或利用 Lucas,Pocklington 和 Proth 的早期结果给出的那些方法. 后面我还要用一节介绍基于递归序列的经典方法.

Wilson 定理可看成是刻画素数的一种聪明的方法，但不能成为实用的方法，因为计算 $(p-1)!$ 是很费时间的.

费马小定理是说：若 p 为素数而 a 不能被 p 整除，则 $a^{p-1}\equiv 1\pmod p$. 但是这个定理的逆不成立, 因为存在合成数 N 和 $a\geqslant 2$, 使得 $a^{N-1}\equiv 1\pmod N$. 我在 2.8 节将会研究这种数 N, 它们在许多素性问题中是非常重要的.

但是 Lucas 于 1876 年发现了费马小定理如下形式的逆是对的：

素性判定 1 设 $N>1$. 如果存在整数 $a>1$, 使得

(i) $a^{N-1}\equiv 1\pmod N$；

(ii) $a^m\not\equiv 1\pmod N$ $(m=1,2,\cdots,N-2)$.

则 N 为素数.

这个方法看似完美，但也有缺点：它需要 $N-2$ 次不断地乘 a, 运算次数太大.

证明 只需证明对每个整数 m $(1 \leqslant m < N)$ 均与 N 互素，即 $\varphi(N) = N-1$. 为此，又只需证明存在 a $(1 \leqslant a < N)$, $\gcd(a,N) = 1$, 使得 a 模 N 的阶为 $N-1$. 这正相当于我们的判定条件. □

1891 年， Lucas 又给出下面的方法：

素性判定 2 设 $N > 1$. 如果存在整数 $a > 1$, 使得

(i) $a^{N-1} \equiv 1 \pmod N$;

(ii) 对每个 $m < N$ 和 $m \mid N-1$, 均有 $a^m \not\equiv 1 \pmod N$.

则 N 为素数.

这个方法的缺点是需要知道 $N-1$ 的全部因子. 这只对 $N-1$ 容易分解的情形有效，如 $N = 2^n + 1$ 或者 $N = 3 \cdot 2^n + 1$.

它的证明和判定 1 的证法是一样的.

1967 年， Brillhart 和 Selfridge 给出比 Lucas 更灵活的方法，还可见 Brillhart,Lehmer 和 Selfridge1975 年的文章.

素性判定 3 设 $N > 1$. 如果对 $N-1$ 的每个素因子 q, 均存在整数 $a = a(q) > 1$, 使得

(i) $a^{N-1} \equiv 1 \pmod N$;

(ii) $a^{\frac{N-1}{q}} \not\equiv 1 \pmod N$.

则 N 为素数.

这个方法的缺点仍是需要知道 $N-1$ 的所有素因子，但是需

要计算的同余式个数有所减少.

善于观察的读者会注意到：在验证 $a^{N-1} \equiv 1 \pmod{N}$ 时，必须对每个 $n \leqslant N-1$ 依次计算 a^n 模 N 的剩余，但这不就把 Lucas 的素性判定 1 作完了吗？关键在于：在计算 a^n 和它模 N 剩余时不需要依次计算所有 a 的方幂，存在下面介绍的一种快速算法. 将 n 按二进制展开

$$n = n_0 2^k + n_1 2^{k-1} + \cdots + n_{k-1} 2 + n_k$$

其中每个 n_i 为 0 或 1, 而 $n_0 = 1$. 如下依次定义整数 $r_0, r_1, r_2, \cdots$ 其中 $r_0 = a$, 而对每个 $j \geqslant 0$

$$r_{j+1} = \begin{cases} r_j^2, & n_{j+1} = 0 \\ a r_j^2, & n_{j+1} = 1 \end{cases}$$

则 $a^n = r_k$.

所以只需最多 $2k$ 次运算, 每次运算为平方或乘 a. 计算 $a^n \pmod{N}$ 甚至更为容易：在每一步可将 r_j 代之以模 N 的剩余. 现在 k 等于

$$\left[\frac{\lg n}{\lg 2}\right]$$

所以若 $n = N-1$, 则只需要大约

$$2\left[\frac{\lg N}{\lg 2}\right]$$

次运算即可求出 $a^{N-1} \pmod{N}$, 不需要把所有 $a^n \pmod{N}$ $(1 \leqslant n \leqslant N-1)$ 都算出来.

请你用此法计算 $2^{1092} \pmod{1093^2}$. 如果没有算错的话，应当是 $2^{1092} \equiv 1 \pmod{1093^2}$. 这个同余式和素性判定没有直接关系，但是在第五章又会见到它.

现在回到 Brillhart 和 Selfridge 的素性判定 3, 给出它的证明.

素性判定 3 的证明 只需证 $\varphi(N) = N-1$. 由于 $\varphi(N) \leqslant N-1$, 只需证 $N-1 \mid \varphi(N)$. 如果这不成立, 则有素数 q 和 $r \geqslant 1$, 使得 $q^r \mid N-1$ 但是 $q^r \nmid \varphi(N)$. 令 $a = a(q)$ 而 e 为 a 模 N 的阶, 则 $e \mid N-1$ 但是 $e \nmid (N-1)/q$, 从而 $q^r \mid e$. 由 $a^{\varphi(N)} \equiv 1 \pmod N$ 可知 $e \mid \varphi(N)$, 于是 $q^r \mid \varphi(N)$. 但与假设矛盾, 证毕. □

在讲述费马数的那一节中, 我将对费马数给出 Pepin 素性判定方法, 它是素性判定 3 的直接推论.

为了使素性判定试验更为有效, 希望避免使用 $N-1$ 的所有素因子, 即试验中只需要 $N-1$ 的一部分分解. 在这方面, Pocklington 于 1914 年证明了如下一个简单结果:

设 $N-1 = q^n R$, 其中 q 为素数, $n \geqslant 1$, $q \nmid R$. 如果存在整数 $a > 1$, 使得

(i) $a^{N-1} \equiv 1 \pmod N$;

(ii) $\gcd(a^{(N-1)/q} - 1, N) = 1$.

则 N 的每个素因子均有形式 $mq^n + 1$, 其中 $m \geqslant 1$.

证明 设 p 是 N 的素因子, e 为 a 模 p 的阶, 于是 $e \mid p-1$. 由条件 (ii) 和 $p \mid N$ 可知 $e \nmid (N-1)/q$, 于是 $q \nmid (N-1)/e$. 从而 $q^n \mid e$, 于是 $q^n \mid p-1$. □

上面的结果看起来与其说是素性判定, 不如说更像是分解. 但若每个素因子 $p = mq^n + 1$ 均大于 $\sqrt{N}$, 则 N 为素数. 在 q^n 相

当大时，用此法判定素性不太花时间.

Pocklington 还将他的上述结果更精细化成：

设 $N-1=FR$, $\gcd(F,R)=1$ 并且知道 F 的分解式，假设对 F 的每个素因子 q 都存在整数 $a=a(q)>1$, 使得

(i) $a^{N-1}\equiv 1 \pmod N$;

(ii) $\gcd(a^{(N-1)/q}-1,N)=1$.

则 N 的每个素因子都有形式 $mF+1$, 其中 $m\geqslant 1$.

同样地，若 $F>\sqrt{N}$, 则 N 为素数. 这个结果在证明某些特殊形式数的素性是很有用的. 由它不难推出 Proth(1878) 一个古老的判别法.

素性判定 4 设 $N=2^nh+1$, 其中 h 为奇数而 $2^n>h$. 假如存在整数 $a>1$, 使得 $a^{(N-1)/2}\equiv -1 \pmod N$, 则 N 为素数.

证明 $N-1=2^nh$, 其中 h 为奇数，而 $a^{N-1}\equiv 1 \pmod N$. 由于 N 为奇数，可知 $\gcd(a^{(N-1)/2}-1,N)=1$. 由上面结果可知 N 的每个素因子都有形式 $p=2^nm+1>2^n$. 但是 $N=2^nh+1<2^{2n}$, 从而 $\sqrt{N}<2^n<p$, 即 N 为素数. □

在下面的判定试验中 (用同样记号) 需要知道 R(即 $N-1$ 的未分解部分) 必须没有素因子小于一个给定的界 B. 确切地说：

素性判定 5 设 $N-1=FR$, 其中 $\gcd(F,R)=1$ 并且已知 F 的因子分解， B 满足 $FB>\sqrt{N}$, 而 R 没有小于 B 的素因子. 假如：

(i) 对 F 的每个素因子 q, 均存在素数 $a=a(q)>1$, 使得

$a^{N-1} \equiv 1 \pmod N$ 并且 $\gcd(a^{(N-1)/q} - 1, N) = 1$;

(ii) 存在整数 $b > 1$, 使得 $b^{N-1} \equiv 1 \pmod N$ 并且 $\gcd(b^F - 1, N) = 1$.

则 N 为素数.

证明 设 p 为 N 的素因子, e 为 b 模 N 的阶, 则 $e \mid p-1$ 并且 $e \mid N-1 = FR$. 由于 $e \nmid F$, 可知 $\gcd(e, R) \neq 1$, 从而存在素数 q, 使得 $q \mid e$ 并且 $q \mid R$. 于是 $q \mid p-1$. 但是由 Pocklington 前面的结果, 可知 $F \mid p-1$. 再由 $\gcd(F, R) = 1$ 便知 $qF \mid p-1$. 于是 $p-1 \geqslant qF \geqslant BF > \sqrt{N}$. 由此可知 $p = N$, 从而 N 为素数. □

Brillhart,Lehmer 和 Selfridge(1975) 的文章中还有这些素性判定方法的另一些变化的形式, 用它们可以决定形如 $2^r + 1$ 、 $2^{2r} \pm 2^r + 1$ 、 $2^{2r-1} \pm 2^r + 1$ 的数的素性.

我已经说过多次并且现在再说一次: 这些判定方法都需要知道 $N-1$ 的素因子. 下面用线性递归序列给出的另一些判别法则需要知道 $N+1$ 的素因子.

2.4 Lucas 数列

设 P 和 Q 为非零整数. 考虑多项式 $X^2 - PX + Q$. 它的判别式为 $D = P^2 - 4Q$, 根为 $\alpha, \beta = \dfrac{P \pm \sqrt{D}}{2}$. 于是

$$\alpha + \beta = P, \quad \alpha\beta = Q, \quad \alpha - \beta = \sqrt{D}$$

假设 $D \neq 0$, 则 $D \equiv 0$ 或 $1 \pmod 4$. 定义数列

$$U_n(P,Q) = \frac{\alpha^n - \beta^n}{\alpha - \beta}, \qquad V_n(P,Q) = \alpha^n + \beta^n \qquad (n \geqslant 0)$$

则 $U_0(P,Q)=0,\ U_1(P,Q)=1,\ V_0(P,Q)=2,\ V_1(P,Q)=P.$

数列

$$U(P,Q)=(U_n(P,Q))_{n\geqslant 0},\quad V(P,Q)=(V_n(P,Q))_{n\geqslant 0}$$

叫作结合于 (P,Q) 的 Lucas 数列. Fibonacci,Fermat 和 Pell 等人考虑了一些特殊情形. 关于这种数列已知许多特别的事实, 而一般的理论是 Lucas 在 1878 年美国数学杂志 *American Journal of Mathematics* 第 1 卷中的长文中的首次研究. 文中内容丰富, 将 Lucas 数列和许多有趣的课题 (如三角函数、连分数、求最大公因子辗转相除算法中除法运算次数、素性判定等) 联系起来. 这里讨论 Lucas 数列是着眼于素性判定. 关于和其他课题的联系可见本书后面的参考文献和其他有关文献. 但是我要提醒, 尽管 Lucas 的文章很重要, 但所用方法常常较为复杂并且不十分明了, 建议读 Carmichael 1913 年的文章, 这篇文章改正了一些错误并对一些结果作了推广.

首先注意, 对每个 $n\geqslant 2$ 可验证有递推公式

$$U_n(P,Q)=PU_{n-1}(P,Q)-QU_{n-2}(P,Q)$$
$$V_n(P,Q)=PV_{n-1}(P,Q)-QV_{n-2}(P,Q)$$

所以这是二阶线性递归序列 (每一项线性地依赖于前面两项). 反之, 对于上述的 P 和 Q, 并且 $D=P^2-4Q\neq 0$. 如果 $(W_0,W_1)=(0,1)$ 或 $(2,P)$, 而当 $n\geqslant 2$ 时, $W_n=PW_{n-1}-QW_{n-2}$. 则 Binet(1843) 证明了

$$W_n=\frac{\alpha^n-\beta^n}{\alpha-\beta}\ \text{或}\ \alpha^n+\beta^n\qquad(n\geqslant 0)$$

其中 α 和 β 是多项式 X^2-PX+Q 的两个根. 这是显然的, 因

为数列

$$(W_n)_{n\geqslant 0} \text{ 和 } \left(\frac{\alpha^n-\beta^n}{\alpha-\beta}\right)_{n\geqslant 0} \qquad (\text{或 } (\alpha^n+\beta^n)_{n\geqslant 0})$$

的前两项一致，然后又都满足同样的二阶线性递推关系.

现在介绍发展一般理论之前所得到的主要特殊情形. Fibonacci 所考虑的情形为 $P=1$, $Q=-1$, $U_0=U_0(1,-1)=0$, $U_1=U_1(1,-1)=1$. 这个数列为

$$0,1,1,2,3,5,8,13,21,34,55,89,144,233,$$
$$377,610,987,1597,2584,4181,6765,\cdots$$

这些数最早出现在 Fibonacci 1202 年著作的一个数学问题中. 正是在这本书中将阿拉伯数字第一次介绍到欧洲. 这个数学问题现在许多数学书中均有介绍，讨论兔子的繁殖问题.

与 Fibonacci 数列相伴随的是 Lucas 数列：仍取 $P=1$, $Q=-1$, 而 $V_0=V_0(1,-1)=2$, $V_1=V_1(1,-1)=1$, 从而 Lucas 数列为

$$2,1,3,4,7,11,18,29,47,76,123,199,322,$$
$$521,843,1364,2207,3571,5778,9349,15127,\cdots$$

如果 $P=3$, $Q=2$, 则所得数列为

$$U_n(3,2)=2^n-1,\quad V_n(3,2)=2^n+1\quad (n\geqslant 0)$$

这两个数列使费马度过了许多不眠之夜 (详见 2.6 和 2.7 节). 对应于 $(P,Q)=(2,-1)$ 的数列叫作 Pell 数列，它们是

$$U_n(2,-1): 0,1,2,5,12,29,70,169,408,985,2378,5741,13860,\cdots$$
$$V_n(2,-1): 2,2,6,14,34,82,198,478,1154,2786,6726,16238,39202,\cdots$$

Lucas 注意到数列 $U_n(P,Q)$ 和 $(a^n-b^n)/(a-b)$,$V_n(P,Q)$ 和 (a^n+b^n) $(n\geqslant 0)$ 有许多相似之处，其中 a 和 b 为整数， $a>b\geqslant 1$, $\gcd(a,b)=1$. 取 $(P,Q)=(a+b,ab)$, 则 $D=(a-b)^2\neq 0$, $\alpha=a$, $\beta=b$, 于是

$$U_n(a+b,ab)=\frac{a^n-b^n}{a-b},\qquad V_n(a+b,ab)=a^n+b^n$$

希望能把关于数列 $(a^n-b^n)/(a-b)$, a^n+b^n 的主要结果 (如整除性和素性) 推广到很广的一类 Lucas 数列中去.

先讲一些代数恒等式. 以下简记 $U_n=U_n(P,Q)$, $V_n=V_n(P,Q)$. 我们有如下代数关系:

(4.1) $U_n=PU_{n-1}-QU_{n-2}$ $(n\geqslant 2)$, $\quad U_0=0,\quad U_1=1$

$V_n=PV_{n-1}-QV_{n-2}$ $(n\geqslant 2)$, $\quad V_0=2,\quad V_1=P$

(4.2) $U_{2n}=U_nV_n$

$V_{2n}=V_n-2Q^n$

(4.3) $U_{m+n}=U_mV_n-Q^nU_{m-n}$

$V_{m+n}=V_mV_n-Q^nV_{m-n}$(当$m\geqslant n$)

(4.4) $U_{m+n}=U_mU_{n+1}-QU_{m-1}U_n$

$2V_{m+n}=V_mV_n+DU_mU_n$

(4.5) $DU_n=2V_{n+1}-PV_n$

$V_n=2U_{n+1}-PU_n$

(4.6) $U_n^2=U_{n-1}U_{n+1}+Q^{n-1}$

$V_n^2=DU_n^2+4Q^n$

(4.7) $U_mV_n-U_nV_m=2Q^nU_{m-n}$(当$m\geqslant n$)

$U_mV_n+U_nV_m=2U_{m+n}$

(4.8) $2^{n-1}U_n=\binom{n}{1}P^{n-1}+\binom{n}{3}P^{n-3}D+\binom{n}{5}P^{n-5}D^2+\cdots$

$2^{n-1}V_n=P^n+\binom{n}{2}p^{n-2}D+\binom{n}{4}P^{n-4}D^2+\cdots$

(4.9) 如果 m 为奇数而 $k\geqslant 1$, 则

$$D^{(m-1)/2}U_k^m = U_{km} - \binom{m}{1}Q^k U_{k(m-2)} + \binom{m}{2}Q^{2k}U_{k(m-4)} - \cdots$$
$$\pm \binom{m}{(m-1)/2}Q^{k(m-1)/2}U_k$$
$$V_k^m = V_{km} + \binom{m}{1}Q^k V_{k(m-2)} + \binom{m}{2}Q^{2k}V_{k(m-4)} + \cdots$$
$$+\binom{m}{(m-1)/2}Q^{k(m-1)/2}V_k$$

如果 m 为偶数而 $k \geqslant 1$, 则

$$D^{m/2}U_k^m = \Big[V_{km} - \binom{m}{1}Q^k V_{k(m-2)} + \binom{m}{2}Q^{2k}V_{k(m-4)} - \cdots$$
$$+ (-1)^{m/2}\binom{m}{m/2}Q^{km/2}V_0\Big] - (-1)^{m/2}\binom{m}{m/2}Q^{km/2}$$
$$V_k^m = \Big[V_{km} + \binom{m}{1}Q^k V_{k(m-2)} + \binom{m}{2}Q^{2k}V_{k(m-4)} + \cdots$$
$$+ \binom{m}{m/2}Q^{km/2}V_0\Big] - \binom{m}{m/2}Q^{km/2}$$

$$(4.10)\ U_m = V_{m-1}+QV_{m-3}+Q^2V_{m-5}+\cdots+\begin{cases} Q^{(m-2)/2}P, & m\text{为偶数} \\ Q^{(m-1)/2}, & m\text{为奇数}\end{cases}$$
$$P^m = V_m + \binom{m}{1}QV_{m-2} + \binom{m}{2}Q^2V_{m-4} + \cdots$$
$$+\begin{cases} \binom{m}{m/2}Q^{m/2}, & m\text{为偶数} \\ \binom{m}{(m-1)/2}Q^{(m-1)/2}P, & m\text{为奇数}\end{cases}$$

为了得到进一步性质，我们需要拉格朗日在 1741 年得出的下列恒等式：

$$X^n + Y^n = (X+Y)^n - \frac{n}{1}XY(X+Y)^{n-2}$$
$$+ \frac{n}{2}\binom{n-3}{1}X^2Y^2(X+Y)^{n-4}$$
$$- \frac{n}{3}\binom{n-4}{2}X^3Y^3(X+Y)^{n-6} + \cdots$$
$$+ (-1)^r\frac{n}{r}\binom{n-r+1}{r-1}X^rY^r(X+Y)^{n-2r} \pm \cdots$$

其中求和是对所有 $2r \leqslant n$ 进行的. 注意右边所有系数均为整数.

(4.11) 若 $m \geqslant 1$ 并且 q 为奇数，则

$$\begin{aligned}U_{mq} = D^{(q-2)/2}U_m^q + \frac{q}{1}Q^m D^{(q-3)/2}U_m^{q-2} \\ + \frac{q}{2}\binom{q-3}{1}Q^{2m}D^{(q-5)/2}U_m^{q-4} + \cdots \\ + \frac{q}{r}\binom{q-r+1}{r-1}Q^{mr}D^{(q-2r-1)/2}U_m^{q-2r} + \cdots + \text{最后一项}\end{aligned}$$

而最后一项为

$$\frac{q}{(q-1)/2}\binom{(q-1)/2}{(q-3)/3}Q^{\frac{q-1}{2}m}U_m = qQ^{\frac{q-1}{2}m}U_m$$

现在按证明的次序依次介绍整除性的结果.

(4.12) $U_n \equiv V_{n-1} \pmod{Q}$,　　$V_n \equiv P^n \pmod{Q}$.

提示：用 (4.10) 或用数学归纳法.

(4.13) 设 p 为奇素数，则

$$U_{kp} \equiv D^{\frac{p-1}{2}}U_k \pmod{p}$$

对 $e \geqslant 1$

$$U_{p^e} \equiv D^{\frac{p-1}{2}e} \pmod{p}$$

特别地

$$U_p \equiv \left(\frac{D}{p}\right) \pmod{p}$$

提示：用 (4.9).

(4.14) $V_p \equiv P \pmod{p}$

提示：用 (4.10).

(4.15) 若 $n, k \geqslant 1$, 则 $U_n \mid U_{kn}$

提示：用 (4.3).

(4.16) 若 $n, k \geqslant 1$ 而 k 为奇数，则 $V_n \mid V_{kn}$

提示：用 (4.9).

记号 设 $n \geqslant 2$. 若存在 $r \geqslant 1$ 使得 $n \mid U_r$. 我们把最小的这种整数 r 表示成 $\rho(n) = \rho(n, U)$.

(4.17) 假设 $\rho(n)$ 存在，并且 $\gcd(n, 2Q) = 1$, 则 $n \mid U_k$ 当且仅当 $\rho(n) \mid k$.

提示：用 (4.15) 和 (4.7).

我们将会看到：对许多满足 $\gcd(n, 2Q) = 1$ 的 n(不是全体这种 n),$\rho(n)$ 是存在的.

(4.18) 若 P 和 Q 均为偶数，则 $n \geqslant 2$ 时 U_n 为偶数， $n \geqslant 1$ 时 V_n 为偶数.

若 P 为奇数，Q 为偶数，则 $n \geqslant 1$ 时，U_n 和 V_n 均为奇数.

若 P 为偶数，Q 为奇数，则 $U_n \equiv n \pmod 2$, 而 V_n 为偶数.

若 P 和 Q 均为奇数，则当 $3 \mid n$ 时 U_n 和 V_n 为偶数，否则 U_n 和 V_n 为奇数.

特别地，若 U_n 为偶数，则 V_n 为偶数.

提示：用 (4.12), (4.5), (4.2), (4.6) 和 (4.1).

下面是第一个主要结果，它可看作是费马小定理的推广.

(4.19) 设 p 为奇素数,

若 $p \mid P$, $p \mid Q$, 则对每个 $k > 1$, $p \mid U_k$.

若 $p \mid P$, $p \nmid Q$, 则 $p \mid U_k$ 当且仅当 $2 \mid k$.

若 $p \nmid P$, $p \mid Q$, 则对每个 $k > 1$, $p \nmid U_k$.

若 $p \nmid PQ$, 但是 $p \mid D$, 则 $p \mid U_k$ 当且仅当 $p \mid k$.

若 $p \nmid PQD$, 则 $p \mid U_{\psi(p)}$, 其中 $\psi(p) = p - (D \mid p)$, 而 $(D \mid p)$

是勒让德符号.

证明 若 $p \mid P$ 并且 $p \mid Q$, 由 (4.1) 可知对每个 $k > 1$, $p \mid U_k$.

若 $p \mid P = U_2$, 由 (4.15) 可知对每个 $k \geqslant 1, p \mid U_{2k}$. 再由 $p \nmid Q$ 和 $U_{2k+1} = PU_{2k} - QU_{2k-1}$, 用归纳法即知 $p \nmid U_{2k+1}$.

若 $p \nmid P$, $p \mid Q$, 由归纳法和 (4.1) 可知对每个 $k \geqslant 1$, $p \nmid U_k$.

若 $p \mid PQ$, $p \mid D$, 由 (4.8),$2^{p-1}U_p \equiv 0 \pmod p$, 从而 $p \mid U_p$. 另一方面, 若 $p \nmid n$, 由 (4.8) 知 $2^{n-1}U_n \equiv nP^{n-1} \not\equiv 0 \pmod p$, 于是 $p \nmid U_n$.

最后考虑最有趣的情形 $p \nmid PQD$. 若 $(D \mid p) = -1$, 由 (4.8) 知

$$
\begin{aligned}
2^pU_{p+1} &= \binom{p+1}{1}P^p + \binom{p+1}{3}P^{p-2}D + \cdots + \binom{p+1}{p}PD^{(p-1)/2} \\
&\equiv P + PD^{(p-1)/2} \equiv 0 \pmod p
\end{aligned}
$$

从而 $p \mid U_{p+1}$. 而 $(D \mid p) = 1$, 则存在 C 使得 $P^2 - 4Q = D \equiv C^2 \pmod p$. 于是 $P^2 \not\equiv C^2 \pmod p$ 并且 $p \nmid C$. 由 (4.8) 式以及

$$
\binom{p-1}{1} \equiv -1 \pmod p, \qquad \binom{p-1}{3} \equiv -1 \pmod p, \cdots
$$

可知

$$
\begin{aligned}
2^{p-2}U_{p-1} &= \binom{p-1}{1}P^{p-2} + \binom{p-1}{3}P^{p-4}D + \binom{p-1}{5}P^{p-6}D^2 + \cdots \\
&\quad + \binom{p-1}{p-2}PD^{(p-3)/2} \\
&\equiv -\left(P^{p-2} + P^{p-4}D + P^{p-6}D^2 + \cdots + PD^{(p-3)/2}\right) \\
&\equiv -P\left(\frac{P^{p-1} - D^{(p-1)/2}}{P^2 - D}\right) \equiv -P\frac{P^{p-1} - C^{p-1}}{P^2 - C^2} \equiv 0 \pmod p
\end{aligned}
$$

从而 $p \mid U_{p-1}$. □

如果用前面引进的记号 $\rho(p)$, 则 (4.19) 中的一些结论可重新叙述成:

若 p 为奇素数并且 $p \nmid Q$, 则当 $p \mid P$ 时 $\rho(p)=2$；当 $p \nmid P, p \mid D$ 时 $\rho(p)=p$. 而当 $p \nmid PD$ 时 $\rho(p) \mid \psi(p)$.

注意对后一情形不一定有 $\rho(p)=\psi(p)$. 我在列举 Lucas 数列的主要性质之后，还要回到这个问题.

对于特殊的 Lucas 数列 $U_n(a+1,a)$, 判别式为 $D=(a-1)^2$, 所以若 $p \nmid a(a^2-1)$, 则 $(D \mid p)=1$ 并且 $p \mid U_{p-1}=(a^{p-1}-1)/(a-1)$. 于是 $p \mid a^{p-1}-1$(当 $p \mid a^2-1$ 时这也成立). 由此得到费马小定理.

(4.20) 令 $e \geqslant 1$, $p^e \| U_m$(即指 $p^e \mid U_m$ 但是 $p^{e+1} \nmid U_m$). 则当 $p \nmid k$ 而 $f \geqslant 1$ 时, $p^{e+f} \mid U_{mkp^f}$.

进而若 $p \mid Q$ 并且 $p^e \neq 2$, 则 $p^{e+f} \| U_{mkp^f}$. 而当 $p^e=2$ 时, $2 \| U_{mk}$.

提示：用 (4.19), (4.18), (4.11) 和 (4.6).

现在推广欧拉定理:

若 α 和 β 为 X^2-PX+Q 的根，定义符号

$$\left(\frac{\alpha,\beta}{2}\right)=\begin{cases} 1, & 2 \mid Q \\ 0, & 2 \nmid Q,\ 2 \mid P \\ -1, & 2 \nmid PQ \end{cases}$$

而对 $p \neq 2$, 定义

$$\left(\frac{\alpha,\beta}{p}\right)=\left(\frac{D}{p}\right) \quad (\text{于是当 } p \mid D \text{时}, \left(\frac{\alpha,\beta}{2}\right)=0)$$

对每个素数 p, 令

$$\psi_{\alpha,\beta}(p) = p - \left(\frac{\alpha,\beta}{p}\right)$$

$$\psi_{\alpha,\beta}(p^e) = p^{e-1}\psi_{\alpha,\beta}(p) \qquad (e \geqslant 1)$$

对于 $n = \prod_{p|n} p^e$, 定义 Carmichael 函数

$$\lambda_{\alpha,\beta}(n) = \text{lcm}\{\psi_{\alpha,\beta}(p^e)\} \quad (\text{lcm 表示最小公倍数})$$

再定义广义欧拉函数

$$\psi_{\alpha,\beta}(n) = \prod_{p|n} \psi_{\alpha,\beta}(p^e)$$

于是 $\lambda_{\alpha,\beta}(n) \mid \psi_{\alpha,\beta}(n)$.

容易看出：对每个素数 $p \nmid a$, $\psi_{a,1}(p) = p - 1 = \varphi(p)$. 所以当 $\gcd(a,n) = 1$ 时， $\psi_{a,1}(n) = \varphi(n)$, $\lambda_{a,1}(n) = \lambda(n)$. 这里 $\lambda(n)$ 是 Carmichael 定义的一个函数，见 2.2 节.

下面是欧拉定理的一个推广.

(4.21) 若 $\gcd(n,Q) = 1$, 则 $n \mid U_{\lambda_{\alpha,\beta}(n)}$. 于是 $n \mid U_{\psi_{\alpha,\beta}(n)}$.

提示：用 (4.19) 和 (4.20).

关于数列 $(V_n)_{n\geqslant 1}$ 的整除性则较为复杂. 首先有：

(4.22) 若 $p \nmid 2QD$, 则 $V_{p-(D|p)} \equiv 2Q^{\frac{1}{2}[1-(D|p)]} \pmod p$.

提示：用 (4.5) 、 (4.13) 、 (4.19) 和 (4.14).

由此可得到关于 $U_{\psi(p)/2}$ 和 $V_{\psi(p)/2}$ 的整除性结果：

(4.23) 若 $p \nmid 2QD$, 则

$$p \mid U_{\psi(p)/2} \text{ 当且仅当 } (Q \mid p) = 1$$
$$p \mid V_{\psi(p)/2} \text{ 当且仅当 } (Q \mid p) = -1$$

提示：前者用 (4.2)、(4.6)、(4.22) 和同余式 $(Q \mid p) \equiv Q^{(p-1)/2} \pmod p$. 后者用 (4.2)、(4.9)、前一结论和 (4.6).

在下面结果中假设 $\gcd(P, Q) = 1$.

(4.24) 对每个 $n \geqslant 1$, $\gcd(U_n, Q) = \gcd(V_n, Q) = 1$.

提示：用 (4.12).

(4.25) $\gcd(U_n, V_n) = 1$ 或 2.

提示：用 (4.16) 和 (4.24).

(4.26) 若 $d = \gcd(m, n)$, 则 $U_d = \gcd(U_m, U_n)$.

提示：用 (4.15)、(4.7)、(4.24)、(4.18) 和 (4.6). 证明事实上不容易，需要用 Lucas 数列 $(U_n(V_d, Q^d))_{n \geqslant 0}$.

(4.27) 若 $\gcd(m, n) = 1$, 则 $\gcd(U_m, U_n) = 1$.

(4.28) 若 $d = \gcd(m, n)$, 并且 m/d, n/d 均为奇数，则 $V_d = \gcd(V_m, V_n)$.

提示：证明和 (4.26) 一样.

下面结果与 (4.17) 类似，但需要假设 $\gcd(P, Q) = 1$.

(4.29) 假设 $\rho(n)$ 存在，则 $n \mid U_k \Leftrightarrow \rho(n) \mid k$.

提示：用 (4.15)、(4.24) 和 (4.3).

现在看一个具体情形：取 $P=1, Q=-1, D=5$. 即 U_n 和 V_n 分别为 Fibonacci 数和 Lucas 数. 这时 (4.18) 为

$$p \mid U_{p-1}, \quad \text{若}(5 \mid p)=1 \ (\text{即 } p \equiv \pm 1 \pmod{10})$$
$$p \mid U_{p+1}, \quad \text{若}(5 \mid p)=-1 \ (\text{即 } p \equiv \pm 3 \pmod{10})$$

而 (4.19) 则为

$$p \mid V_{p-1}-2, \quad \text{若}(5 \mid p)=1 \ (\text{即 } p \equiv \pm 1 \pmod{10})$$
$$p \mid V_{p+1}+2, \quad \text{若}(5 \mid p)=-1 \ (\text{即 } p \equiv \pm 3 \pmod{10})$$

Jarden 于 1958 年证明了：对 Fibonacci 数列，函数

$$\frac{\psi(p)}{\rho(p)}=\frac{p-(5 \mid p)}{\rho(p)}$$

在 $p \to \infty$ 时无界. 这个结果由 Kiss 和 Phong 于 1978 年推广为：存在 $C>0$(只依赖于 P 和 Q), 使得当 $p \to \infty$ 时， $\psi(p)/\rho(p)$ 无界，但是 $\psi(p)/\rho(p)<C[p/\lg p]$.

现在讲 Lucas 数列模素数 p 的性质. 若 $p=2$, 则由 (4.18) 所刻画. 例如，当 P 和 Q 均为奇数时，数列 $(U_n)_{n\geqslant 0}$ 和 $(V_n)_{n\geqslant 0}$ 模 2 均为 $0,1,1,0,1,1,0,1,1,0,\cdots$ 以下设 p 为奇素数.

(4.30) 若 $p \nmid 2QD$ 并且 $(D \mid p)=1$, 则

$$U_{n+p-1} \equiv U_n \pmod{p}, \qquad V_{n+p-1} \equiv V_n \pmod{p}$$

所以序列 $(U_n)_{n\geqslant 0}$ 和 $(V_n)_{n\geqslant 0}$ 模 p 均是周期 $p-1$ 的序列.

证明 由 (4.4), $U_{n+p-1}=U_nU_p-QU_{n-1}U_{p-1}$. 由 (4.19), $\rho(p) \mid p-(D \mid p)=p-1$. 由 (4.15),$p \mid U_{p-1}$. 当 $p \mid P$, $p \nmid Q$ 时这也成立，因为 $2 \mid p-1$, 由 (4.19) 可知 $p \mid U_{p-1}$. 再由 (4.13) 知 $U_p \equiv (D \mid p) \equiv 1 \pmod{p}$. 所以 $U_{n+p-1} \equiv U_n \pmod{p}$.

由 (4.5),$V_{n+p-1} \equiv 2U_{n+p} - PU_n \equiv 2U_{n+1} - PU_n \equiv V_n \pmod p$. □

与此相伴随的是下面结果:

(4.31) 设 $p \nmid 2QD$,e 为 Q 模 p 的阶. 如果 $(D \mid p) = -1$, 则

$$U_{n+e(p+1)} \equiv U_n \pmod p, \qquad V_{n+e(p+1)} \equiv V_n \pmod p$$

从而序列 $(U_n)_{n\geqslant 0}$ 和 $(V_n)_{n\geqslant 0}$ 模 p 均是周期 $e(p+1)$ 的序列.

证明 若 $p \nmid P$, 由 (4.19) 和 (4.15) 可知 $p \mid U_{p-(D|p)} = U_{p+1}$. 而这在 $p \mid P$ 时也成立. 由 (4.22) 知 $V_{p+1} \equiv 2Q \pmod p$. 现在对 $r \geqslant 1$ 归纳证明 $V_{r(p+1)} \equiv 2Q^r \pmod p$. 如果这对 r 成立, 则由 (4.4) 有

$$2V_{(r+1)(p+1)} = V_{r(p+1)}V_{p+1} + DU_{r(p+1)}U_{p+1} \equiv 4Q^{r+1} \pmod p$$

从而 $V_{(r+1)(p+1)} \equiv 2Q^{r+1} \pmod p$. 特别有 $V_{e(p+1)} \equiv 2Q^e \equiv 2 \pmod p$. 由 (4.7) 有

$$U_{n+e(p+1)}V_{e(p+1)} - U_{e(p+1)}V_{n+e(p+1)} = 2Q^{e(p+1)}U_n$$

所以 $2U_{n+e(p+1)} \equiv 2U_n \pmod p$. 这就给出第一个同余式. 用 (4.5) 则得到第二个同余式. □

为了总结上述结果, 我们引入集合

$$\mathcal{P}(U) = \{素数\ p \mid 存在\ n\ 使得\ U_n \neq 0 并且 p \mid U_n\}$$

$$\mathcal{P}(V) = \{素数\ p \mid 存在\ n\ 使得\ V_n \neq 0 并且 p \mid V_n\}$$

它们分别是数列 $U = (U_n)_{n\geqslant 1}$ 和 $V = (V_n)_{n\geqslant 1}$ 的素因子集合. 以下设 P 和 Q 是互素的非零整数, 并且判别式 $D = P^2 - 4Q \neq 0$.

第一种情形是存在 $n>1$, 使得 $U_n=0$. 这相当于 $\alpha^n=\beta^n$, 从而 α/β 是单位根. 若 n 是使 $U_n=0$ 成立的最小正整数, 则当 $1\leqslant r\leqslant n-1$ 时, $U_r\neq 0$. 而对每个 $k\geqslant 1, U_{nk+r}=\alpha^{nk}U_r$. 于是 $\mathcal{P}(U)$ 即是 $U_2\cdots U_{n-1}$ 的所有素因子组成的集合. 类似可知 $\mathcal{P}(V)$ 即是 $V_1V_2\cdots V_{n-1}V_n$ 的全部素因子组成的集合.

如果 α/β 不是单位根, 则对每个 $n\geqslant 1$, $U_n\neq 0$, $V_n\neq 0$. 这时由 (4.18) 和 (4.19) 可知 $\mathcal{P}(U)=\{$素数 $p\mid p\nmid Q\}$. 特别对于 Fibonacci 数列, $\mathcal{P}(U)$ 是全体素数所组成的集合.

对于 Lucas 数列 $V=(V_n)_{n\geqslant 1}$ 则不能得到这样精细的结果. 由 $U_{2n}=U_nV_n$ $(n\geqslant 1)$ 可知 $\mathcal{P}(V)$ 为 $\mathcal{P}(U)$ 的子集合. 由 (4.18) 可知: $2\in\mathcal{P}(V)$ 当且仅当 $2\nmid Q$. 对于 $p\neq 2$, 由 (4.24) 和 (4.6) 可知在 $p\mid DQ$ 时 $p\notin\mathcal{P}(V)$; 而在 $p\nmid 2DQ$ 并且 $(Q\mid p)=-1$ 时 $p\in\mathcal{P}(V)$(见 (4.23)); 另一方面, 若 $p\nmid 2DQ, (Q\mid p)=1$ 并且 $(D\mid p)=-(-1\mid p)$, 则 $p\notin\mathcal{P}(V)$. 如果 $p\nmid 2DQ, (Q\mid p)=1$ 并且 $(D\mid p)=(-1\mid p)$, 则需要进一步分析才能决定 p 是否属于 $\mathcal{P}(V)$. 但无论如何, 已知 $\mathcal{P}(V)$ 是一个无限集合.

对于 Lucas 数列 $(P=1,Q=-1,D=5)$, 上面事实可更清楚地叙述成

$$\text{当 } p\equiv 3,7,11,19 \pmod{20}\text{时, } p\in\mathcal{P}(V)$$

$$\text{当 } p\equiv 13,17 \pmod{20}\text{时, } p\notin\mathcal{P}(V)$$

当 $p\equiv 1,9 \pmod{20}$ 时, Ward 于 1961 年作了更仔细研究. Jarden 在 1958 年就证明了: 存在无穷多 $p\equiv 1 \pmod{20}$, 使得 $p\notin\mathcal{P}(V)$, 并且也存在无穷多 $p\equiv 1 \pmod{40}$, 使得 $p\in\mathcal{P}(V)$.

我在第五章 5.8 节会进一步研究集合 $\mathcal{P}(U)$ 和 $\mathcal{P}(V)$, 考虑它们对于全体素数集合的密度.

类比于 Bang 和 Zsigmondy 定理, Carmichael 考虑关于参数

(P,Q) 的 Lucas 数列的本原素因子. p 叫作 U_k(或 V_k) 的本原素因子，是指 $p \mid U_k(p \mid V_k)$, 但是当 $l < k$ 时， $p \nmid U_l(p \nmid V_l)$.

Zsigmondy 定理的证明并不容易，下面是一些精细结果.

Carmichael 证明了：若判别式 $D > 0$, 则对每个 $n \neq 1, 2, 6$, 除了情形 " $P = \pm 1, Q = -1, n = 12$ " 之外， U_n 均有本原素因子. 又若 D 为平方数，则对每个 n, 除了情形 " $P = \pm 3, Q = 2, n = 6$ " 之外， U_n 均有本原素因子.

你能看出第二个论断包含 Zsigmondy 定理吗？若 $P = 1$, $Q = -1$, 则例外情形即是 Fibonacci 数 $U_{12} = 144$.

对于伴随序列，如果 $D > 0$, 则对每个 $n \neq 1, 3$, 除了情形 " $n = 6, P = \pm 1, Q = -1$ " (即 Lucas 数 $V_6 = 18$) 之外， V_n 均有本原素因子. 又若 D 是平方数，则例外情形只有 " $n = 3, P = \pm 3, Q = 2$ "，这个例外包含在 Zsigmondy 定理之中.

但是当 $D < 0$ 时，这类结果不再成立. Carmichael 已注意到 $P = 1, Q = 2$ 的情形，这时对于 $n = 1, 2, 3, 5, 8, 12, 13$ 和 18, U_n 都没有本原素因子.

Schinzel 在 1962 年证明了以下结果.

设 $(U_n)_{n \geqslant 0}$ 是对于互素参数 (P,Q) 的 Lucas 数列，并且 $D < 0$. 又设 α/β 不是单位根，则均存在有效可计算的 n_0(依赖于 P 和 Q), 使得当 $n \geqslant n_0$ 时， U_n 均有本原素因子.

Schinzel 于 1974 年又给出一个重要的结果，即上述结果中的 n_0 可以取为绝对常数. 利用 Baker 方法， Stewart 于 1977 年证明了：若 $n > e^{452}2^{67}$, 则 U_n 有本原素因子. Stewart 还证明了：对任意给定的 $n(n \neq 6, n > 4)$, 只存在有限多个可以明确决定的 Lucas 数列，使得 U_n 没有本原素因子.

表 2.2 Fibonacci 数和 Lucas 数 ($P = 1,\ \ Q = -1$)

Fibonacci 数	Lucas 数
$U(0) = 0\ \ U(1) = 1$	$V(0) = 2\ \ V(1) = 1$
$U(2) = 1$	$V(2) = 3$
$U(3) = 2$	$V(3) = 4$
$U(4) = 3$	$V(4) = 7$
$U(5) = 5$	$V(5) = 11$
$U(6) = 8$	$V(6) = 18$
$U(7) = 13$	$V(7) = 29$
$U(8) = 21$	$V(8) = 47$
$U(9) = 34$	$V(9) = 76$
$U(10) = 55$	$V(10) = 123$
$U(11) = 89$	$V(11) = 199$
$U(12) = 144$	$V(12) = 322$
$U(13) = 233$	$V(13) = 521$
$U(14) = 377$	$V(14) = 843$
$U(15) = 610$	$V(15) = 1364$
$U(16) = 987$	$V(16) = 2207$
$U(17) = 1597$	$V(17) = 3571$
$U(18) = 2584$	$V(18) = 5778$
$U(19) = 4181$	$V(19) = 9349$
$U(20) = 6765$	$V(20) = 15127$
$U(21) = 10946$	$V(21) = 24476$
$U(22) = 17711$	$V(22) = 39603$
$U(23) = 28657$	$V(23) = 64079$
$U(24) = 46368$	$V(24) = 103682$
$U(25) = 75025$	$V(25) = 167761$
$U(26) = 121393$	$V(26) = 271443$
$U(27) = 196418$	$V(27) = 439204$
$U(28) = 317811$	$V(28) = 710647$
$U(29) = 514229$	$V(29) = 1149851$
$U(30) = 832040$	$V(30) = 1860498$
$U(31) = 1346269$	$V(31) = 3010349$
$U(32) = 2178309$	$V(32) = 4870847$
$U(33) = 3524578$	$V(33) = 7881196$
$U(34) = 5702887$	$V(34) = 12752043$
$U(35) = 9227465$	$V(35) = 20633239$
$U(36) = 14930352$	$V(36) = 33385282$
$U(37) = 24157817$	$V(37) = 54018521$
$U(38) = 39088169$	$V(38) = 87403803$
$U(39) = 63245986$	$V(39) = 141422324$
$U(40) = 102334155$	$V(40) = 228826127$

表 2.3　数 2^n-1和 $2^n+1(P=3,\ Q=2)$

2^n-1	2^n+1
$U(0)=0\ \ U(1)=1$	$V(0)=2\ \ V(1)=3$
$U(2)=3$	$V(2)=5$
$U(3)=7$	$V(3)=9$
$U(4)=15$	$V(4)=17$
$U(5)=31$	$V(5)=33$
$U(6)=63$	$V(6)=65$
$U(7)=127$	$V(7)=129$
$U(8)=255$	$V(8)=257$
$U(9)=511$	$V(9)=513$
$U(10)=1023$	$V(10)=1025$
$U(11)=2047$	$V(11)=2049$
$U(12)=4095$	$V(12)=4097$
$U(13)=8191$	$V(13)=8193$
$U(14)=16383$	$V(14)=16385$
$U(15)=32767$	$V(15)=32769$
$U(16)=65535$	$V(16)=65537$
$U(17)=131071$	$V(17)=131073$
$U(18)=262143$	$V(18)=262145$
$U(19)=524287$	$V(19)=524289$
$U(20)=1048575$	$V(20)=1048577$
$U(21)=2097151$	$V(21)=2097153$
$U(22)=4194303$	$V(22)=4194305$
$U(23)=8388607$	$V(23)=8388609$
$U(24)=16777215$	$V(24)=16777217$
$U(25)=33554431$	$V(25)=33554433$
$U(26)=67108863$	$V(26)=67108865$
$U(27)=134217727$	$V(27)=134217729$
$U(28)=268435455$	$V(28)=268435457$
$U(29)=536870911$	$V(29)=536870913$
$U(30)=1073741823$	$V(30)=1073741825$
$U(31)=2147483647$	$V(31)=2147483649$
$U(32)=4294967295$	$V(32)=4294967297$
$U(33)=8589934591$	$V(33)=8589934593$
$U(34)=17179869183$	$V(34)=17179869185$
$U(35)=34359738367$	$V(35)=34359738369$
$U(36)=68719476735$	$V(36)=68719476737$
$U(37)=137438953471$	$V(37)=137438953473$
$U(38)=274877906943$	$V(38)=274877906945$
$U(39)=549755813887$	$V(39)=549755813889$
$U(40)=1099511627775$	$V(40)=1099511627777$

表 2.4　Pell 数 ($P=2,\quad Q=-1$)

Pell 数	伴随 Pell 数
$U(0)=0\quad U(1)=1$	$V(0)=2\quad V(1)=2$
$U(2)=2$	$V(2)=6$
$U(3)=5$	$V(3)=14$
$U(4)=12$	$V(4)=34$
$U(5)=29$	$V(5)=82$
$U(6)=70$	$V(6)=198$
$U(7)=169$	$V(7)=478$
$U(8)=408$	$V(8)=1154$
$U(9)=985$	$V(9)=2786$
$U(10)=2378$	$V(10)=6726$
$U(11)=5741$	$V(11)=16238$
$U(12)=13860$	$V(12)=39202$
$U(13)=33461$	$V(13)=94642$
$U(14)=80782$	$V(14)=228486$
$U(15)=195025$	$V(15)=551614$
$U(16)=470832$	$V(16)=1331714$
$U(17)=1136689$	$V(17)=3215042$
$U(18)=2744210$	$V(18)=7761798$
$U(19)=6625109$	$V(19)=18738638$
$U(20)=15994428$	$V(20)=45239074$
$U(21)=38613965$	$V(21)=109216786$
$U(22)=93222358$	$V(22)=263672646$
$U(23)=225058681$	$V(23)=636562078$
$U(24)=543339720$	$V(24)=1536796802$
$U(25)=1311738121$	$V(25)=3710155682$
$U(26)=3166815962$	$V(26)=8957108166$
$U(27)=7645370045$	$V(27)=21624372014$
$U(28)=1845756052$	$V(28)=52205852194$
$U(29)=44560482149$	$V(29)=126036076402$
$U(30)=107578520350$	$V(30)=304278004998$
$U(31)=259717522849$	$V(31)=734592086398$
$U(32)=627013566048$	$V(32)=1773462177794$
$U(33)=1513744654945$	$V(33)=4281516441986$
$U(34)=3654502875938$	$V(34)=10336495061766$
$U(35)=8822750406821$	$V(35)=24954506565518$
$U(36)=21300003689580$	$V(36)=60245508192802$
$U(37)=51422757785981$	$V(37)=145445522951122$
$U(38)=124145519261542$	$V(38)=351136554095046$
$U(39)=299713796309065$	$V(39)=847718631141214$
$U(40)=723573111879672$	$V(40)=2046573816377474$

表 2.5　数 $U(4,3)$和 $V(4,3)$($P=4$,　$Q=3$)

数 $U(n)$	伴随数 $V(n)$
$U(0)=0$　$U(1)=1$	$V(0)=2$　$V(1)=4$
$U(2)=4$	$V(2)=10$
$U(3)=13$	$V(3)=28$
$U(4)=40$	$V(4)=82$
$U(5)=121$	$V(5)=244$
$U(6)=364$	$V(6)=730$
$U(7)=1093$	$V(7)=2188$
$U(8)=3280$	$V(8)=6562$
$U(9)=9841$	$V(9)=19684$
$U(10)=29524$	$V(10)=59050$
$U(11)=88573$	$V(11)=177148$
$U(12)=265720$	$V(12)=531442$
$U(13)=797161$	$V(13)=1594324$
$U(14)=2391484$	$V(14)=4782970$
$U(15)=7174453$	$V(15)=14348908$
$U(16)=21523360$	$V(16)=43046722$
$U(17)=64570081$	$V(17)=129140164$
$U(18)=193710244$	$V(18)=387420490$
$U(19)=581130733$	$V(19)=1162261468$
$U(20)=1743392200$	$V(20)=3486784402$
$U(21)=5230176601$	$V(21)=10460353204$
$U(22)=15690529804$	$V(22)=31381059610$
$U(23)=47071589413$	$V(23)=94143178828$
$U(24)=141214768240$	$V(24)=282429536482$
$U(25)=423644304721$	$V(25)=847288609444$
$U(26)=1270932914164$	$V(26)=2541865828330$
$U(27)=3812798742493$	$V(27)=7625597484988$
$U(28)=11438396227480$	$V(28)=22876792454962$
$U(29)=34315188682441$	$V(29)=68630377364884$
$U(30)=102945566047324$	$V(30)=205891132094650$
$U(31)=308836698141973$	$V(31)=617673396283948$
$U(32)=926510094425920$	$V(32)=1853020188851842$
$U(33)=2779530283277761$	$V(33)=5559060566555524$
$U(34)=8338590849833284$	$V(34)=16677181699666570$
$U(35)=25015772549499853$	$V(35)=50031545098999708$
$U(36)=75047317648499560$	$V(36)=150094635296999122$
$U(37)=225141952945498681$	$V(37)=450283905890997364$
$U(38)=675425858836496044$	$V(38)=1350851717672992090$
$U(39)=2026277576509488133$	$V(39)=4052555153018976268$
$U(40)=6078832729528464400$	$V(40)=12157665459056928802$

另一个有趣问题是考虑 U_n 的本原部分 U_n^*, 它定义为

$$U_n = U_n^* U_n', \qquad \gcd(U_n^*, U_n') = 1$$

并且 $p \mid U_n^*$ 当且仅当 p 是 U_n 的本原素因子.

Schinzel 于 1963 年给出存在两个 (甚至两个以上) 本原素因子的一些条件. 由这些条件可以推出：若 $D > 0$, 或者 $D < 0$ 并且 α/β 不是单位根，则有无穷多个 n, 使得 U_n^* 为合成数.

何时 U_n^* 无平方因子？这是一个很难的问题. 对于 $P = 3, Q = 2$ 这一特别情形，序列为 $U_n = 2^n - 1$, 这个问题都很困难 (见 2.2 节的评论).

2.5 基于 Lucas 数列的素性检测

这件事由 Lucas 开始，由 Lehmer 继续，再被后人改进. 用此法对 N 作素性检测，需要知道 $N+1$ 的素因子. 而在第 2.3 节采用的方法则需要 $N-1$ 的素因子. 我们这里的工具是 Lucas 序列. 根据 (4.18), 若 N 是奇素数，而 $U = (U_n)_{n \geqslant 0}$ 是判别式为 D 的 Lucas 序列. 如果 $N \nmid DPQ$, 则 $N \mid U_{N-(D|N)}$. 特别若雅可比符号 $(D \mid N) = -1$, 则 $N \mid U_{N+1}$.

但是要注意，我在第 2.3 节指出其逆不成立，因为存在合成数 N 和判别式为 D 的 Lucas 序列 $(U_n)_{n \geqslant 0}$, 使得 $N \mid U_{N-(D|N)}$. 我们将在第 2.10 节研究这样的数.

为方便起见，对每个整数 $D > 1$, 定义如下的函数 ψ_D. 如果 $N = \prod_{i=1}^{s} p_i^{e_i}$, 令

$$\psi_D(N) = \frac{1}{2^{s-1}} \prod_{i=1}^{s} p_i^{e_i - 1} \left(p_i - \left(\frac{D}{p_i} \right) \right)$$

注意若 $(U_n)_{n \geqslant 0}$ 是判别式为 D 的 Lucas 序列， α 和 β 是所结合

多项式的根，则第 2.4 节中考虑的函数 $\psi_{\alpha,\beta}$ 和 ψ_D 之间的关系为

$$\psi_{\alpha,\beta}(N) = 2^{s-1}\psi_D(N)$$

由于需要同时考虑具有相同判别式 D 的多个 Lucas 序列，所以最好是采用 ψ_D 而不是对应不同序列的不同函数 $\psi_{\alpha,\beta}$. 比如若 $U(P,Q)$ 的判别式为 D, 则对于 $P' = P+2$, $Q' = P+Q+1$, $U(P',Q')$ 的判别式也为 D.

我们从一些简单结果开始.

(5.1) 若 $2 \nmid N$, $\gcd(N,D) = 1$, 则 $\psi_D(N) = N - (D \mid N)$ 当且仅当 N 为素数.

证明 若 N 为素数，由定义 $\psi_D = N - (D \mid N)$, 若 $N = p^e$, 其中 p 为素数而 $e \geqslant 2$, 则 $\psi_D(N)$ 是 p 的倍数而 $N - (D \mid N)$ 不是. 若 $N = \prod_{i=1}^{s} p_i^{e_i}$ 而 $s \geqslant 2$, 则由 $N > 5$ 可知

$$\begin{aligned}\psi_D(N) &\leqslant \frac{1}{2^{s-1}}\prod_{i=1}^{s} p_i^{e_i-1}(p_i+1) = 2N\prod_{i=1}^{s}\frac{1}{2}\left(1+\frac{1}{p_i}\right)\\ &\leqslant 2N\cdot\frac{2}{3}\cdot\frac{3}{5}\cdots\leqslant\frac{4N}{5} < N-1\end{aligned}$$ □

(5.2) 若 $2 \nmid N$, $\gcd(N,D) = 1$ 并且 $N - (D \mid N) \mid \psi_D(N)$, 则 N 为素数.

证明 设 N 为合成数. 先设 $N = p^e$, 其中 p 为素数而 $e \geqslant 2$. 则 $\psi_D(N) = p^e - p^{e-1}(D \mid p)$, 所以

$$p^e - p^{e-1} < p^e - 1 \leqslant N - (D \mid N) \leqslant \psi_D(N) = p^e - p^{e-1}(D \mid p).$$

这表明 $(D \mid p) = -1$ 并且 $N - (D \mid N) = p^e \pm 1$ 除尽 $\psi_D(N) = p^e + p^{e-1} = p^e \pm 1 + (p^{e-1} \mp 1)$, 而这是不可能的.

若 N 有多于 1 个不同的素因子，由 (5.1) 知 $\psi_D(N) < N-1 \leqslant N-(D \mid N)$，这也和假设相矛盾．因此 N 为素数．

(5.3) 若 $2 \nmid N$，$U = U(P,Q)$ 是判别式为 D 的 Lucas 序列，$\gcd(N,QD)=1$．则 $N \mid U_{\psi_D(N)}$．

证明　由 $\gcd(N,Q)=1$ 和 (4.12) 可知 $N \mid \lambda_{\alpha,\beta}(N)$，其中 α 和 β 为 X^2-PX+Q 的根．如果 $N=\prod_{i=1}^{s} p_i^{e_i}$，则

$$\begin{aligned}\lambda_{\alpha,\beta}(N) &= \gcd\left\{p_i^{e_i-1}\left(p_i-\left(\frac{D}{p_i}\right)\right)\right\}\\ &= 2\gcd\left\{\frac{1}{2}p_i^{e_i-1}\left(p_i-\left(\frac{D}{p_i}\right)\right)\right\}\end{aligned}$$

从而 $\lambda_{\alpha,\beta}(N)$ 除尽

$$2\prod_{i=1}^{s}\frac{1}{2}p_i^{e_i-1}\left(p_i-\left(\frac{D}{p_i}\right)\right)=\psi_D(N)$$

由 (4.15) 可知 $n \mid U_{\psi_D(N)}$．

(5.4) 若 $2 \nmid N$，$U=U(P,Q)$ 是判别式为 D 的 Lucas 序列，$(D \mid N)=-1$，$N \mid U_{N+1}$，则 $\gcd(N,QD)=1$．

证明　由于 $(D \mid N) \neq 0$，可知 $\gcd(N,D)=1$．如果 N 和 Q 有公共素因子 p，由 $p \nmid D=P^2-4Q$ 可知 $p \nmid P$．由 (4.18) 可知对每个 $n \geqslant 1$，$p \nmid U_n$．而这与假设矛盾，所以 $\gcd(N,Q)=1$．

我们还需要如下一个结果．

(5.5) 设 $2 \nmid N$，q 为 $N+1$ 的素因子，$U=U(P,Q)$ 和 $V=V(P,Q)$ 是对于 (P,Q) 的 Lucas 序列，判别式 $D \neq 0$．又设 $\gcd(P,Q)=1$ 或者 $\gcd(N,Q)=1$．如果 N 除尽 $U_{(N+1)/q}$ 和 $V_{(N+1)/2}$，则 $N \mid V_{(N+1)/2q}$．

证明 $\frac{N+1}{2}=\frac{N+1}{2q}+\frac{N+1}{q}u$, 其中 $u=\frac{q-1}{2}$ 由 (4.4) 可知

$$2V_{(N+1)/2}=V_{(N+1)/2q}V_{[(N+1)/q]u}+DU_{(N+1)/2q}U_{[(N+1)/q]u}.$$

由 (4.15),$N\mid U_{[(N+1)/q]u}$, 所以 $N\mid V_{(N+1)/2q}V_{[(N+1)/q]u}$.

如果 $\gcd(P,Q)=1$, 由 (4.21),$\gcd\left(U_{[(N+1)/q]u},\ V_{[(N+1)/q]u}\right)=1$ 或 2. 所以 $\gcd(N,V_{[(N+1)/q]u})=1$, 从而 $N\mid V_{(N+1)/2q}$. 如果 $\gcd(N,Q)=1$, 假设 N 和 $V_{[(N+1)/q]u}$ 有公共素因子 p, 由 (4.6), $p\mid 4Q$. 从而 $p\mid Q$(因为 p 是奇素数), 这导致矛盾. □

在介绍素性检测之前，我们给出一个数为合成数的一些充分性条件.

设 $N>1$ 为奇整数. 如果存在参数为 (P,Q) 的 Lucas 序列 $(U_n)_{n\geqslant 0}$, 判别式为 D, 并且 $\gcd(N,QD)=1$, $(Q\mid N)=1$, 而且 $N\nmid U_{\frac{1}{2}[N-(D|N)]}$. 则 N 是合成数.

类似地，若存在参数为 (P,Q) 的 Lucas 伴随序列 $(V_n)_{n\geqslant 0}$, 判别式为 D, 并且 $N\nmid QD$, $(Q\mid N)=-1$, 而且 $n\nmid V_{\frac{1}{2}[N-(D|N)]}$, 则 N 为合成数.

证明 若 $N=p$ 是奇素数, $p\nmid QD$. 若 $(Q\mid p)=1$, 则 $p\mid U_{\psi(p)/2}$. 若 $(Q\mid p)=-1$, 则 $p\mid V_{\psi(p)/2}$(参见 (4.23)). 两种情形均导致矛盾. □

现在给出一批素性检测方法, 每种方法都比前一个方法要好.

检测 1 设 $N>1$ 为奇素数, $N+1=\prod_{i=1}^{s}q_i^{f_i}$. 如果存在整数 D, 使得 $(D\mid N)=-1$, 并且对 $N+1$ 的每个素因子 q_i, 都有判别式 $D=P_i^2-4Q_i$ 的 Lucas 序列 $(U_n^{(i)})_{n\geqslant 0}$, 满足 $\gcd(P_i,Q_i)=1$ 或者 $\gcd(N,Q_i)=1$. 使得 $N\mid U_{N+1}^{(i)}$, $N\nmid U_{(N+1)/q_i}^{(i)}$, 则 N 为

素数.

这个检测的缺点是需要 $N+1$ 的所有素因子，并且对 $n=1,2,\cdots,N+1$ 要计算 $U_n^{(i)}$.

证明 由 (5.3) 和 (5.4) 可知对每个 $i=1,\cdots,s$, $N \mid U_{\psi_D(N)}^{(i)}$. 记 $\rho^{(i)}(N)$ 为最小整数 r 使得 $N \mid U_r^{(i)}$. 由 (4.29) 或者 (4.22) 以及假设条件，可知 $\rho^{(i)}(N) \mid (N+1)$, $\rho^{(i)}(N) \nmid (N+1)/q_i$, $\rho^{(i)}(N) \mid \psi_D(N)$. 由此可知对每个 $i=1,\cdots,s$, $q_i^{f_i} \mid \rho^{(i)}(N)$. 于是 $(N+1) \mid \psi_D(N)$. 再由 (5.2) 知 N 是素数. □

下面的检测方法把计算量减少一半.

检测 2 设 $N>1$ 为奇数, $N+1=\prod_{i=1}^s q_i^{f_i}$. 假设存在整数 D 使得 $(D \mid N)=-1$, 并且对 $N+1$ 的每个素因子 q_i, 均存在判别式为 $D=P_i^2-4Q_i$ 的 Lucas 序列 $(V_n^{(i)})_{n\geqslant 0}$, 其中 $\gcd(P_i,Q_i)=1$ 或者 $\gcd(N,Q_i)=1$, 并且 $N \mid V_{(N+1)/2}^{(i)}$, $N \nmid V_{(N+1)/2q_i}^{(i)}$. 则 N 为素数.

证明 由 (4.2) 知 $N \mid U_{N+1}^{(i)}$. 由 (5.5) 知 $N \nmid U_{(N+1)/q_i}^{(i)}$. 再由检测 1 知 N 为素数. □

下面的检测只需要 $N+1$ 的一部分素因子.

检测 3 设 $N>1$ 为奇数, q 为 $N+1$ 的一个素因子，并且 $2q>\sqrt{N}+1$. 假设存在判别式 $D=P^2-4Q$ 的 Lucas 序列 $(V_n)_{n\geqslant 0}$, 其中 $\gcd(P,Q)=1$ 或者 $\gcd(N,Q)=1$, 并且 $(D \mid N)=-1$, $N \mid V_{(N+1)/2}$, $N \nmid V_{(N+1)/2q}$. 则 N 是素数.

这个检测的缺点是需要 $N+1$ 的一个足够大的素因子.

证明 设 $N=\prod_{i=1}^s p_i^{e_i}$. 由 (4.2) 知 $N \mid U_{N+1}$. 然后由 (4.29) 或 (4.22) 可知 $\rho(N) \mid (N+1)$. 由 (5.5) 知 $N \nmid U_{(N+1)/q}$, 所以 $\rho(N) \nmid (N+1)/q$. 这表明 $q \mid \rho(N)$. 由 (5.4) 和 (5.3) 知 $N \mid U_{\psi_D(N)}$,

所以 $\rho(N) \mid \psi_D(N)$, 这给出 $\rho(N) \mid N \cdot \prod_{i=1}^{s}(p_i - (D \mid p_i))$.

由于 $q \nmid N$, 可知存在 p_i 使得 $q \mid p_i - (D \mid p_i)$. 于是 $p_i \equiv (D \mid p_i) \pmod{2q}$. 这给出 $p_i \geqslant 2q - 1 > \sqrt{N}$, $1 \leqslant N/p_i < \sqrt{N} < 2q - 1$. 所以 $N/p_i = 1$, 即 N 为素数. □

下面的检测是由 Morrison 于 1975 年提出的, 可看成是第 2.3 节中 Pocklington 检测的一个类比.

检测 4 设 $N > 1$ 为奇数, $N + 1 = FR$, $\gcd(F, R) = 1$, 并且知道 F 的素因子分解式. 又设存在整数 D 使得 $(D \mid N) = -1$, 并且对 F 的每个素因子 q_i, 均存在判别式为 $D = P_i^2 - 4Q_i$ 的 Lucas 序列 $(U_n^{(i)})_{n \geqslant 0}$, 其中 $\gcd(P_i, Q_i) = 1$ 或者 $\gcd(N, Q_i) = 1$, 使得$N \mid U_{N+1}^{(i)}$, $\gcd(U_{(N+1)/q_i}^{(i)}, N) = 1$. 则对 N 的每个素因子 p, 均有 $p \equiv (D \mid p) \pmod{F}$. 又若 $F > \sqrt{N} + 1$, 则 N 是素数.

证明 由假设知 $\rho^{(i)}(N) \mid (N+1)$, 于是 $\rho^{(i)}(p) \mid (N+1)$. 但是 $p \nmid U_{(N+1)/q_i}^{(i)}$, 所以由 (4.29) 或 (4.22),$\rho^{(i)}(p) \nmid (N+1)/q_i$. 如果 $q_i^{f_i} \| F$, 则 $q_i^{f_i} \mid \rho^{(i)}(p)$. 由 (4.18) 可知 $q_i^{f_i} \mid p - (D \mid p)$, 这可推出$F \mid p-(D \mid p)$. 又若 $F > \sqrt{N} + 1$, 则 $p + 1 \geqslant p - (D \mid p) \geqslant F > \sqrt{N} + 1$. 所以 $p > \sqrt{N}$. 这表明 N 为素数. □

下面结果告诉我们 N 可能有的素因子.

(5.6) 设 N 为奇数, $N + 1 = FR$, $\gcd(F, R) = 1$, 并且知道 F 的素因子分解式. 假设存在判别式为 $D = P^2 - 4Q$ 的 Lucas 序列 $(U_n)_{n \geqslant 0}$, 其中 $\gcd(P, Q) = 1$ 或者 $\gcd(N, Q) = 1$, 使得 $(D \mid N) = -1$, $N \mid U_{N+1}$ 并且 $\gcd(U_F, N) = 1$. 如果 p 是 N 的素因子, 则存在 R 的素因子 q, 使得 $p \equiv (D \mid p) \pmod{q}$.

证明 由 (4.18) 和 $\rho(p) \mid (N+1)$ 可知 $\rho(p) \mid p - (D \mid p)$. 但是 $p \nmid U_F$, 所以 $\rho(p) \nmid F$. 于是 $\gcd(\rho(p), R) \neq 1$. 所以 $\rho(p)$ 和 R 有公

共素因子 q . 特别有 $p\equiv(D\mid p)\pmod q$. □

这个结果给出以下检测方法.

检测 5 设 $N>1$ 为奇数, $N+1=FR$, $\gcd(F,R)=1$, 并且知道 F 的素因子分解式. 而 R 没有比 B 小的素因子, 其中 $BF>\sqrt{N}+1$. 如果存在 D 使得 $(D\mid N)=-1$ 并且满足以下两个条件:

(i) 对 F 的每个素因子 q_i, 都有判别式为 $D=P_i^2-4Q_i$ 的 Lucas 序列 $(U_n^{(i)})_{n\geqslant 0}$, 其中 $\gcd(P_i,Q_i)=1$ 或者 $\gcd(N,Q_i)=1$, 使得 $N\mid U_{N+1}^{(i)}$ 并且 $\gcd(U_{(N+1)/q_i}^{(i)},N)=1$.

(ii) 存在判别式为 $D=P'^2-4Q'$ 的 Lucas 序列 $(U'_n)_{n\geqslant 0}$, 其中 $\gcd(P',Q')=1$ 或者 $\gcd(N,Q')=1$, 使得 $N\mid U'_{N+1}$ 并且 $\gcd(U'_F,N)=1$, 则 N 为素数.

证明 设 p 为 N 的素因子. 由检测 4 知 $p\equiv(D\mid p)\pmod F$. 而由 (5.6) 知存在 R 的素因子 q, 使得 $p\equiv(D\mid p)\pmod q$. 于是 $p\equiv(D\mid p)\pmod{qF}$. 这时

$$p+1\geqslant p-(D\mid p)\geqslant qF\geqslant BF>\sqrt{N}+1$$

所以 $p>\sqrt{N}$. 由于 p 是 N 的任意素因子, 可知 N 必为素数. □

检测 5 比前面的检测都更灵活, 因为只需要 $N+1$ 的一部分因子, 只要使 $N+1$ 的另一部分没有小于 B 的因子即可.

现在我想说明如何快速计算 Lucas 序列中的项 U_n 和 V_n, 其中的 n 很大. 这里有一种方法与第 2.3 节计算高次方幂的方法相类似.

设 $n=n_0 2^k+n_1 2^{k-1}+\cdots+n_k$ 为 n 的二进制展开, 其中 $n_i\in\{0,1\}$, $n_0=1$, 于是 $k=[\lg n/\lg 2]$. 为了计算 U_n(或 V_n), 需

要对一些 m 同时计算 U_m 和 V_m. 需要以下的公式:

$$\begin{cases} U_{2j} = U_j V_j \\ V_{2j} = V_j^2 - 2Q^j \end{cases} \qquad (\text{见 (4.2) 式})$$

$$\begin{cases} 2U_{2j+1} = V_{2j} + PU_{2j} \\ 2V_{2j+1} = PV_{2j} + DU_{2j} \end{cases} \qquad (\text{见 (4.5) 式})$$

令 $s_0 = n_0 = 1$, $s_{j+1} = 2s_j + n_{j+1}$. 则 $s_k = n$. 所以只需对 $j \leqslant k$ 计算 U_{s_j} 和 V_{s_j}. 注意

$$U_{s_{j+1}} = U_{2s_j+n_{j+1}} = U_{2s_j} \text{ 或 } U_{2s_j+1}$$

$$V_{s_{j+1}} = V_{2s_j+n_{j+1}} = V_{2s_j} \text{ 或 } V_{2s_j+1}$$

所以只需算 $4k$ 个数, 即 $2k$ 个 U_i 和 $2k$ 个 V_i. 如果只需知道 $U_n \pmod N$, 则每步计算都可把一个数改用模 N 的最小正剩余.

第二种方法也很快. 对于 $j \geqslant 1$

$$\begin{pmatrix} U_{j+1} & V_{j+1} \\ U_j & V_j \end{pmatrix} = \begin{pmatrix} P & -Q \\ 1 & 0 \end{pmatrix} \begin{pmatrix} U_j & V_j \\ U_{j-1} & V_{j-1} \end{pmatrix}$$

令 $M = \begin{pmatrix} P & Q \\ 1 & 0 \end{pmatrix}$, 则

$$\begin{pmatrix} U_n & V_n \\ U_{n-1} & V_{n-1} \end{pmatrix} = M^{n-1} \begin{pmatrix} U_1 & V_1 \\ 0 & 2 \end{pmatrix}$$

为求 M^m, 将 m 表成二进制, 然后可像计算一个数的 m 次方那样计算 M^m. 如果只需计算 $U_n \pmod N$, 则上面计算的每一步可随时把数改用它模 N 的最小正剩余.

在本小节的结尾, 我想指出: 还有很多其他类似的素性检测方法适用于某种形式的数. 这些方法采用 Lucas 序列或者其他类似的序

列. 有时可以组合使用第 2.3 节中的检测和本节的检测方法, 见 Brillhart, Lehmer 和 Selfridge(1975) 文章. 我想再 (半开玩笑地) 作一点评论: 一般来说, 检测程序叙述得愈长, 素性判定执行起来往往愈快.

以上所介绍的检测方法可用于形如 $2^n - 1$ 的数 (例如第 2.7 节的 Mersenne 数, 那里给出更具体的检测方法), 也可用于形如 $k \cdot 2^n - 1$ 的数 (见 Inkeri 1960 年文章或 Riesel 1985 年的书).

1998 年, H.C.Williams 出版了一本书, 对 Lucas 的工作进行了历史性的数学研究. 读者若想了解更多, 我推荐去看这本权威性并且介绍更详细的著作.

2.6 费马数

对于具有更特别形式的数, 则有更适宜的方法来判别它们是素数还是合成数. 比如对形如 $2^m + 1$ 的数的研究就有很长的历史了.

如果 $2^m + 1$ 为素数, 则 $m = 2^n$, 即必为费马数 $F_n = 2^{2^n} + 1$. 前几个费马数 $F_0 = 3, F_1 = 5, F_2 = 17, F_3 = 257, F_4 = 65537$ 都是素数. 费马相信并且打算证明: 所有费马数都是素数. 由于 F_5 是 10 位数, 为了检测它的素性, 需要在 10^5 以内的素数表 (当时费马没有这种数据), 或者采用某种判别法, 能够判别某个数是否为费马数的因子. 在这些方面费马都没有成功.

欧拉证明了: 当 $n \geqslant 2$ 时, F_n 的每个因子必有形式 $k \cdot 2^{n+2} + 1$, 由此他找到了 F_5 的一个素因子 641

$$F_5 = 641 \times 6700417$$

证明 只需证 F_n 的每个素因子 p 有所述形式. 由于 $2^{2^n} \equiv -1 \pmod{p}$, 可知 $2^{2^{n+1}} \equiv 1 \pmod{p}$. 所以 2 模 p 的阶为 2^{n+1}. 由

费马小定理知 $2^{n+1} \mid p-1$. 特别地, $8 \mid p-1$. 于是 $2^{(p-1)/2} \equiv (2 \mid p) = 1 \pmod{p}$. 所以又有 $2^{n+1} \mid \dfrac{p-1}{2}$. 这表明 $p = k \cdot 2^{n+2} + 1$. □

当 n 增大时, F_n 增大的很快, 所以判别 F_n 的素性很花时间. 利用 Lucas 给出的费马小定理逆命题, Pepin 在 1877 年对于费马数给出以下判定素性的方法.

Pepin 检测 令 $F_n = 2^{2^n} + 1$ $(n \geqslant 2)$, $k \geqslant 2$. 则以下两条件等价.

(i) F_n 为素数并且 $(k \mid F_n) = -1$.

(ii) $k^{(F_n-1)/2} \equiv -1 \pmod{F_n}$.

证明 如果 (i) 成立, 则由欧拉判别法

$$k^{(F_n-1)/2} \equiv \left(\frac{k}{F_n}\right) \equiv -1 \pmod{F_n}$$

反之若 (ii) 成立, 取 $1 \leqslant a < F_n$ 使得 $a \equiv k \pmod{F_n}$. 则 $a^{(F_n-1)/2} \equiv -1 \pmod{F_n}$. 于是 $a^{F_n-1} \equiv 1 \pmod{F_n}$. 由第 2.3 节的检测 3,$F_n$ 为素数. 而且

$$\left(\frac{k}{F_n}\right) \equiv k^{(F_n-1)/2} \equiv -1 \pmod{F_n}$$ □

可以取 $k = 3, 5, 10$. 由于 $F_n \equiv 2 \pmod{3}$, $F_n \equiv 2 \pmod{5}$, $F_n \equiv 1 \pmod{8}$, 利用雅可比互反律得到

$$\left(\frac{3}{F_n}\right) = \left(\frac{F_n}{3}\right) = \left(\frac{2}{3}\right) = -1$$

$$\left(\frac{5}{F_n}\right) = \left(\frac{F_n}{5}\right) = \left(\frac{2}{5}\right) = -1$$

$$\left(\frac{10}{F_n}\right) = \left(\frac{2}{F_n}\right) = \left(\frac{5}{F_n}\right) = -1$$

这个检测在应用中很有效，但若 F_n 为合成数，这个检测不能给出 F_n 的任何因子.

Lucas 用这个方法证明了 F_6 是合成数. 而 Landry 在 82 岁的时候 (1880 年) 给出分解式

$$F_6 = 274177 \times 67280421310721$$

Landry 没有说明他如何给出这个分解式. Williams(1993) 根据 Landry 的信件和文章中的一些线索，指出了 Landry 所用的方法. 但是在 Biermann(1964) 为 Clausen 所写的传记中有一个更精彩的故事. Clausen 是著名的计算能手和天文学家，他在 1855 年 1 月 1 日给高斯的信中已经得到 F_6 的完全分解式. 这封信保存在哥丁根大学图书馆中. Clausen 在信中相信，F_6 的两个因子中的大因子是当时所知的最大素数. 奇怪的是，Biermann 在传记知所写的有关评注多年来并不为人所知.

将费马数因子分解是一个被大量研究的课题. 表 2.6 中给出这项研究的现状，其中 P_n 表示是一个 n 位的素数，而 C_n 表示一个 n 位的合成数.

表 2.6　费马数的完全分解式

$$F_5 = 641 \times 6700417$$
$$F_6 = 274177 \times 67280421310721$$
$$F_7 = 59649589127497217 \times 5704689200685129054721$$
$$F_8 = 1238926361552897 \times P62$$
$$F_9 = 2424833 \times 7455602825647884208337395736200454918783366342657 \times P99$$
$$F_{10} = 45592577 \times 6487031809 \times 4659775785220018543264560743076778192897 \times P252$$
$$F_{11} = 319489 \times 974849 \times 167988556341760475137 \times 3560841906445833920513 \times P564$$

注记

F_5: 欧拉 (1732)

F_6: 第 1 个因子由 Clausen(1855, 未公开发表),Landry 和 Le Lasseur(1880)

F_7: Morrison 和 Brillhart(1970)

F_8: Brent 和 Pollard(1980), 第 1 个因子

F_9: Western(1903), 第 1 个因子; 其余因子由 A.K.Lenstra 和 Manasse(1990)

F_{10}: 第 1 个因子由 Selfridge(1953), 第 2 个因子由 Brillhart (1962) 其余因子由 Brent(1995)

F_{11}: 前两个因子由 Cunningham(1899), 其余因子由 Brent (1988) 第 5 个因子的素性由 Morain(1988) 证明.

跟踪迅速发展的所有最新结果和了解费马数分解的最新方法是相当困难的. 在这些方面, Brent(1999) 和 Brent, Crandall, Dilcher 和 van Halewyn(2000) 的文章包含许多信息. 作者感谢 W.Keller 使其能跟上关于费马数研究进展的步伐 (见表 2.7 、 2.8).

表 2.7 费马数的不完全分解

$$F_{12} = 114689 \times 26017793 \times 63766529 \times 190274191361 \times 1256132134125569 \times C1187$$

$$F_{13} = 2710954639361 \times 2663848877152141313 \times 3603109844542291969 \times 319546020820551643220672513 \times C2391$$

$$F_{15} = 1214251009 \times 2327042503868417 \times 168768817029516972383024127016961 \times C9808$$

$$F_{16} = 825753601 \times 188981757975021318420037633 \times C19694$$

$$F_{17} = 31065037602817 \times C39444$$

$$F_{18} = 13631489 \times 81274690703860512587777 \times C78884$$

$$F_{19} = 70525124609 \times 646730219521 \times C157804$$

$$F_{21} = 4485296422913 \times C631294$$

$$F_{23} = 167772161 \times C2525215$$

表 2.8　费马数是合成数，但不知它的素因子

F_{14}：	Selfridge and Hurwitz (1963)
F_{20}：	Buell and Young (1987)
F_{22}：	Crandall, Doenias, Norrie and Young (1993)
	Carvalho and Trevisan (1993)(彼此独立地)
F_{24}：	Mayer, Papadopoulos and Crandall (1999)

目前完全不了解的最小费马数为 $F_{33}, F_{34}, F_{35}, F_{40}, F_{41}, F_{44}, \cdots$

记录

A. 目前所知的最大费马数为 $F_4 = 65537$.

B. 目前所知为合成数的最大费马数是 $F_{2145351}$，它有因子$3 \cdot 2^{2145353} + 1$. 这个 645817 位的因子是 J.B.Cosgrave 和他在 St.Patrick 学院 (爱尔兰；都柏林) 的研究小组于 2003 年 2 月 21 日找到的. P.Jobling,G.Woltman 和 Y.Gallot 三人的研究计划在这项发现中起了本质的作用.

C. 到 2003 年 5 月底，已知共有 214 个费马数是合成数.

下面是一些未解的问题：

1) 是否存在无穷多费马素数？

由于高斯的一个著名结果，这个问题成为一个重要的问题. 高斯在《算术探究》一书的第 365 、 366 两节解决了古代三大数学难题之一：哪些正 n 边形 $(n \geqslant 3)$ 可以尺规作图？他证明了：可以尺规作图的正多边形的边数有形式 $n = 2^k p_1 \cdots p_h$，其中 $k, h \geqslant 0$，而 $p_1, \cdots, p_h$ 是不同的费马素数.

1844 年， Eisenstein 曾经想证明存在无穷多个费马素数. 事实上，早在 1828 年，一位不知名的作者说过：

$$2+1,\ \ 2^2+1,\ \ 2^{2^2}+1,\ \ 2^{2^{2^2}}+1, \cdots$$

都是素数，并且还认为再加上 $2^{2^3}+1$ 之后就给出全部费马素数. 但是 Selfridge 在 1953 年发现 F_{16} 的一个因子，即 F_{16} 不是素数，从而否定了上述猜想.

2) 是否存在无穷多费马数是合成数？

使用目前的方法，似乎很难解决这两个问题，至今我们对它们还所知甚少.

3) 是否每个费马数都是无平方数 (即没有大于 1 的平方因子)？

Lehmer 和 Schinzel 都猜想有无穷多个费马数没有平方因子. 设 p 为素数，而 p^2 除尽某个费马数，不难证明 $2^{p-1}\equiv 1 \pmod{p^2}$. 我将在第五章 5.3 节给出证明. 由于费马数是彼此互素的，如果存在无穷多个有平方因子的费马数，则存在无穷多个素数 p 满足上述同余式. 我将在第五章讨论这个同余式. 满足这个同余式的素数 p 是不多的. 特别地，现在不知道是否有无穷多素数满足这个同余式.

Sierpiński 在 1958 年研究数 $S_n=n^n+1\ (n\geqslant 2)$. 他证明了：若 S_n 为素数，则存在 $m\geqslant 0$, 使得 $n=2^{2^m}$, 所以 $S_n=F_{m+2^m}$ 是费马数. 由此可证明：在位数 $\leqslant 3\cdot 10^{20}$ 的整数中，S_n 为素数的只有 5 和 257. 这两个数对应于 $m=0$ 和 $1(F_1=5, F_3=257)$. 对于 $m=2,3,4,5, F_6, F_{11}, F_{20}$ 和 F_{37} 都是合成数. 对于 $m=6$ 则为 F_{70}, 目前不知 F_{70} 是否为素数，但是

$$F_{70}>2^{2^{70}}>2^{10^{21}}=(2^{10})^{10^{20}}>10^{3\cdot 10^{20}}$$

形如 n^n+1 的素数是很少的. 但是，是否只有有限多个这种形式的素数？如果答案是肯定的，那就有无穷多费马数为合成数. 但是这个猜想没有任何基础.

最近三位作者 (Krizek, Luca 和 Somer) 合写一本 257 页的

书，书名叫《关于费马大数的 17 个讲义》，书中介绍了费马数的一些有趣的事情. 由于费马数研究进展得迅速，我在这里向读者提出一个问题：下一本关于费马数的书要有多少页？

2.7 Mersenne 数

如果 2^m-1 为素数，则 $m=q$ 必为素数. 并且还不难证明：若 2^m-1 是一个素数的方幂，则 2^m-1 必为素数，从而 m 为素数 (如果你不能证明这件事，请看 Ligh 和 Neal(1974) 的文章).

数 $M_q=2^q-1$(q 为素数) 叫作 Mersenne 数，考虑这种数是源于对于完全数的研究 (见本节附录).

在 Mersenne 那个时代就已经知道某些 Mersenne 数为素数，另一些为合成数. 例如，$M_2=3, M_3=7, M_5=31, M_7=127$ 为素数，而 $M_{11}=23\times 89$. 1640 年，Mersenne 说对于 $q=13,17,19,31,67,127$ 和 257，M_q 均是素数. 但是对于 $q=67$ 和 257，他说得不对，并且在 $q\leqslant 257$ 时，$q=61,89$ 和 107 时，M_q 也是素数. 既使如此，由于这些数都很大，他的论断还是令人惊讶.

要判别一个 Mersenne 数是否为素数，显然需要有办法决定它的因子. 在这方面，欧拉在 1750 年叙述了一个古典结果，它由 Lagrange(1775) 和 Lucas(1878) 所证明.

若 $q\equiv 3 \pmod 4$ 为素数，则 $2q+1 \mid M_q$ 当且仅当 $2q+1$ 为素数. 并且在 $2q+1$ 为素数时，若 $q>3$，则 M_q 为合成数.

证明 令 $n=2q+1 \mid M_q$. 由于 $2^2\not\equiv 1 \pmod n$，可知 $2^q\not\equiv 1 \pmod n$，$2^{2q}-1=(2^q+1)M_q\equiv 0 \pmod n$. 由第 2.3 的 Lucas 检测 3 可知 n 是素数. 反之若 $p=2q+1$ 为素数. 由于 $p\equiv$

$7 \pmod 8$), $(2 \mid p) = 1$, 所以有整数 m, 使得 $2 \equiv m^2 \pmod p$. 于是 $2^q \equiv 2^{(p-1)/2} \equiv m^{p-1} \equiv 1 \pmod p$, 即 $p \mid M_q$.

又若 $q > 3$, 则 $M_q = 2^q - 1 > 2q + 1 = p$. 从而 M_q 是合成数.

□

这表明对于 $q = 11, 23, 83, 131, 179, 191, 239$ 和 251,M_q 分别有因子 $23, 47, 167, 263, 359, 383, 479$ 和 503.

大约在 1825 年, Sophie Germain 考虑 q 和 $2q+1$ 同为素数这件事和费马猜想之间的联系. 这样的素数 q 现在叫作 Sophie Germain 素数. 我将在第五章讨论这种素数.

容易决定 Mersenne 素数的因子所具有的形式.

若 $n \mid M_q$ $(q > 2)$, 则 $n \equiv \pm 1 \pmod 8$ 并且 $n \equiv 1 \pmod q$.

证明 只需对 M_q 的每个素因子 p 证明所述性质. 若 $p \mid M_q = 2^q - 1$, 则 $2^q \equiv 1 \pmod q$. 由费马小定理知 $q \mid p-1$, 即 $p - 1 = 2kq$(由于 $p \neq 2$). 于是

$$\left(\frac{2}{p}\right) \equiv 2^{\frac{p-1}{2}} \equiv 2^{qk} \equiv 1 \pmod p$$

由第 2.2 节所述的勒让德符号性质, 可知 $p \equiv \pm 1 \pmod 8$. □

Cataldi 用试除法证明了 M_{13} 和 M_{17} 为素数, 欧拉也是用试除法证明了 M_{31} 为素数, 但是前面所述关于 Mersenne 数因子的形式, 可知欧拉做了许多计算. 对此可见 Williams 和 Shallit(1994) 的文章.

就目前所知, 判别 M_q 是否为素数的最好方法, 是由 Lucas(1878) 和 Lehmer(1930, 1935) 指明的基于一种递归序列的计算. 还可见 Western(1932), Hardy 和 Wright(1938) 和 Kaplansky(1945). 但是

用此法不能明显地得到 M_q 的因子.

如果 $2 \nmid n \geqslant 3$, 则 $M_n = 2^n - 1 \equiv 7 \pmod{12}$. 又若 $N \equiv 7 \pmod{12}$, 则雅可比符号

$$\left(\frac{3}{N}\right) = \left(\frac{N}{3}\right)(-1)^{(N-1)/2} = -1$$

关于 Mersenne 数的素性检测 令 $P = 2$, $Q = -2$, 考虑它对应的 Lucas 序列 $(U_m)_{m\geqslant 0}$ 和 $(V_m)_{m\geqslant 0}$. 它们的判别式为 $D = 12$. 则 $N = M_n$ 为素数当且仅当 $N \mid V_{(N+1)/2}$.

证明 若 N 为素数，由 (4.2)

$$\begin{aligned} V_{(N+1)/2}^2 &= V_{N+1} + 2Q^{(N+1)/2} = V_{N+1} - 4(-2)^{(N-1)/2} \\ &\equiv V_{N+1} - 4\left(\frac{-2}{N}\right) \equiv V_{N+1} + 4 \pmod{N} \end{aligned}$$

这是因为 $N \equiv 3 \pmod 4$ 和 $N \equiv 7 \pmod 8$, 可知

$$\left(\frac{-2}{N}\right) = \left(\frac{-1}{N}\right)\left(\frac{2}{N}\right) = -1$$

只需再证 $V_{N+1} \equiv -4 \pmod{N}$.

由 (4.4),$2V_{N+1} = V_N V_1 + DU_N U_1 = 2V_N + 12U_N$. 再由 (4.14) 和 (4.13)

$$V_{N+1} = V_N + 6U_N \equiv 2 + 6(12 \mid N) \equiv 2 - 6 \equiv -4 \pmod{N}$$

反之设 $N \mid V_{(N+1)/2}$, 由 (4.2) 知 $N \mid V_{N+1}$. 又由 (4.6),$V_{(N+1)/2}^2 - 12U_{(N+1)/2}^2 = 4(-1)^{(N+1)/2}$, 从而 $\gcd(N, U_{(N+1)/2}) = 1$. 又有 $\gcd(N, 2) = 1$, 由第 2.5 节检测 1 可知 N 为素数. □

为了计算简单，更方便的是将序列 $(V_m)_{m\geqslant 0}$ 改用由

$$S_0 = 4, \qquad S_{k+1} = S_k^2 - 2$$

递归定义的序列 $(S_k)_{k\geqslant 0}$. 此序列为 $4, 14, 194, \cdots$. 而检测为

$$M_n = 2^n - 1 \text{ 是素数当且仅当 } M_n \mid S_{n-2}$$

证明 $S_0 = 4 = V_2/2$. 设 $S_{k+1} = V_{2^k}/2^{2^{k-1}}$, 则

$$S_k = S_{k-1}^2 - 2 = \frac{V_{2^k}^2}{2^{2^k}} - 2 = \frac{V_{2^{k+1}} + 2^{2^{k+1}}}{2^{2^k}} - 2 = \frac{V_{2^{k+1}}}{2^{2^k}}$$

由上述检测即知

$$M_n\text{为素数} \Leftrightarrow M_n \mid V_{(M_n+1)/2} = V_{2^{n-1}} = 2^{2^{n-2}} S_{n-2} \Leftrightarrow M_n \mid S_{n-2}$$

□

这个检测的优点是计算可以依次进行. 所有大的 Mersenne 素数都是用这种方法发现的. Lucas 本人在 1876 年证明了 M_{127} 是素数, 而 M_{67} 为合成数. 不久以后 Pervushin 证明了 M_{61} 也是素数. 最后 Lehmer 于 1927 年证明了 M_{257} 为合成数 (发表于 1932 年). 注意 M_{127} 是 39 位数, 是计算机时代之前所发现的最大素数. 它作为世界记录保持了很长一段时间.

$q \leqslant 127$ 的 Mersenne 素数都是在计算机时代之前发现的. 图灵 (A.Turing) 在 1951 年第一个试图用电子计算机寻找 Mersenne 素数, 但他没有成功. Robinson 用一个 SWAC 计算机在洛杉矶美国国家标准局进行 Lehmer 检测方法. 在 D.H.Lehmer 和 E.Lehmer 协助之下, 于 1952 年 1 月 30 日第一次用计算机发现了 M_{521} 和 M_{607} 为素数. 在同一年后来又找到素数 M_{1279}, M_{2203} 和 M_{2281}.

当 q 很大时, 用 Lucas-Lehmer 试验法判别 M_q 的素性需要很大的计算量, 一定要由一个团队在高速计算机上工作. 而且采用专门设计的程序. 在做乘法运算时, Schönhage 和 Strassen 于

1971 年发明的快速傅里叶变换起了重要作用. 在寻找大素数时出现了 Crandall 和 Woltman 的研究计划.

由 Woltman 组织的 "寻找 Mersenne 素数的互联网计划" (great internet mersenne prime search, GIMPS), 目的是寻找大的 Mersenne 素数. 任何人只要愿意, 都可带上个人电脑参加这个计划, 他将会收到软件和一些素指数, 这是他的工作领域. 现在这项计划已登记了几千位参加者.

距现在不算太久远, 那些淘金者们离开家庭和朋友, 闯过蟒蛇遍布的丛林和疾病蔓延的沼泽, 走向无人居住的荒野或悬崖峭壁的雪山, 去寻找财富. 寻找 Mersenne 素数的现代探索者们做着类似的探险. 他们不能预见自己所猎取目标的位置, 首先找到信息的人靠的是运气好, 但不能使他致富. 现实情况和我的这个比喻没有多大差别, 读者可以参看 Woltman(1999) 描述他自己发现第 38 个 Mersenne 素数的历程: 探险队长说……

记录

表 2.9 中列出前 38 个 Mersenne 素数. 目前所知的最大的Mersenne 素数为 M_q, $q = 13466917$. 这个素数有 4053946 位. 它是由 M. Cameron, G. F. Woltman 和 S. Kurowski 根据 GIMPS 研究项目于 2001 年 11 月 14 日发现的. 这是目前所知的最大素数. 一百万位以上的 "超级素数" 现在只知道两个.

素数 M_{110503} 是在 M_{132049} 和 M_{216091} 之后发现的. 下一个 Mersenne 素数可能会在 $q < 13466917$ 范围内找到, 因为对这个范围以内的素数 q, 还有许多 M_q 没有确定它们的素性.

另一方面, 我们已经说过, 若 $q = k \cdot 2^N - 1$ 为 Sophie Germain 素数 (即 q 和 $2q+1$ 均为素数), 则 M_q 是合成数.

表 2.9　Mersenne 素数 $M_q, q < 7000000$

q	发现时间 (年)	发现者
2	-	-
3	-	-
5	-	-
7	-	-
13	1461	未知 *
17	1588	P.A.Cataldi
19	1588	P.A.Cataldi
31	1750	L.Euler
61	1883	I.M.Pervushin
89	1911	R.E.Powers
107	1913	E.Fauquenmbergue
127	1876	E.Lucas
521	1952	R.M.Robinson
607	1952	R.M.Robinson
1279	1952	R.M.Robinson
2203	1952	R.M.Robinson
2281	1952	R.M.Robinson
3217	1957	H.Riesel
4253	1961	A.Hurwitz
4423	1961	A.Hurwitz
9689	1963	D.B.Gillies
9941	1963	D.B.Gillies
11213	1963	D.B.Gillies
19937	1971	B.Tuckerman
21701	1978	L.C.Noll and L.Nickel
23209	1979	L.C.Noll
44497	1979	H.Nelson and D.Slowinski
86243	1982	D.Slowinski
110503	1988	W.N.Colquitt and L.Welsh, Jr.
132049	1983	D.Slowinski
216091	1985	D.Slowinski
756839	1992	D.Slowinski and P.Gage
859433	1993	D.Slowinski and P.Gage
1257787	1996	D.Slowinski and P.Gage
1398269	1996	J.Armengaud, G.F.Woltman and GIMPS
2976221	1997	G.Spence, G.F.Woltman and GIMPS
3021377	1998	R.Clarkson, G.F.Woltman, S.Kurowski and GIMPS
6972593	1999	N.Hajratwala, G.F.Woltman, S.Kurowski and GIMPS

* 见 Dickson 《数论史》第一卷第 6 页.

记录

目前已知最大的合成数 M_q 为 $q = 2540041185 \times 2^{114729} - 1$，由 D.Underbakke, G.F.Woltman 和 Y.Gallot 于 2003 年 1 月发现. 这个 q 是目前所知最大的 Sophie Germain 素数 (见第五章 5.2 节).

Riesel 的书 (1985) 中有 $M_n = 2^n - 1$ $(2 \nmid n \leqslant 257)$ 的完全分解表. 更大的表请见 Brillhart 等人于 1983 年、1988 年和 2002 年 (第 3 版) 出版的著作.

像费马数一样，对于 Mersenne 数也有许多问题.

(1) 是否存在无穷多 Mersenne 素数？

(2) 是否存在无穷多 Mersenne 数为合成数？

这两个问题的答案应当都是肯定的，我将解释为什么会这样. 比如，在第六章第 6.1 节，在 (D5) 之后可以看到：在一个类似于 Mersenne 数的序列中包含有无穷多个合成数.

(3) 是否每个 Mersenne 数都无平方因子？

Rotkiewicz 在 1965 年证明了：若 p 为素数而 p^2 除尽某个 Mersenne 数，则 $2^{p-1} \equiv 1 \pmod{p^2}$. 当费马数被 p^2 除尽时，已经得到过类似的同余式.

关于 Mersenne 数还想再提两个问题，其中一个已经解决，另一个则至今未解决.

如果 M_q 为素数，那么 M_{M_q} 是否一定也是素数？

答案是否定的： $M_{13} = 8191$ 为素数，而 M_{8191} 为合成数，这是由 Wheeler 证明的，见 Robinson (1954) 的论文. 注意 M_{8191} 是多于 2400 位的数字. 1976 年， Keller 找到了 M_{8191} 的一个素因子：

$$p = 2 \times 20644229 \times M_{13} + 1 = 338193759479$$

由此给出 M_{8191} 是合成数的一个简单证明：为了验证 $2^{2^{13}} \equiv 2 \pmod{p}$，只需计算 13 个模 p 的平方运算. 这是 Keller 写信告诉我的.

第 2 个问题是 Catalan 在 1876 年建议的，可见 Dickson 《数论史》第 1 卷第 22 页. 考虑数列

$$\begin{aligned}
C_1 &= 2^2 - 1 = 3 = M_2 \\
C_2 &= 2^{C_1} - 1 = 7 = M_3 \\
C_3 &= 2^{C_2} - 1 = 127 = M_7 \\
C_4 &= 2^{C_3} - 1 = 2^{127} - 1 = M_{127} \\
&\vdots \\
C_{n+1} &= 2^{C_n} - 1 \\
&\vdots
\end{aligned}$$

是否这些数 C_n 都是素数？其中是否有无穷多个素数？目前连 C_5 都无法试验，因为它有 10^{37} 位！

最后介绍 Bateman,Selfridge 和 Wagstsff(1989) 关于 Mersenne 素数的一个有趣的猜想.

猜想 设 p 为正奇数 (不必为素数). 若下面条件中有两个成立，则第三个条件也成立.

(a) $p = 2^k \pm 1$ 或者 $4^k \pm 3$(对某个 $k \geqslant 1$).

(b) M_p 为素数.

(c) $(2^p+1)/3$ 为素数.

H.Lifchitz 和 R.Lifchitz 在私人通信中告诉我这个猜想对于 $p < 720000$ 均对. 在这个范围内, 满足这三个条件的素数只有 $p = 3, 5, 7, 13, 17, 19, 31, 61, 127$. 人们相信也只有它们是满足这三个条件的素数.

附录：关于完全数

现在我介绍完全数, 讲述它们与 Mersenne 数的关系.

自然数 $n > 1$ 叫作完全数, 是指它等于所有小于它的正因子之和, 例如, 在 10000 以内的完全数有 $n = 6, 28, 496, 8128$.

在古代人们就知道完全数. 神学和宗教作家把第一个完全数 6 和完美性联系在一起, 创世需要 6 天, 所以世界是完美的.

欧几里得在他的《几何原本》第九章命题 36 中证明了：若 q 为素数而 $M_q = 2^q - 1$ 为素数, 则 $N = 2^{q-1}(2^q - 1)$ 是完全数. 欧拉后来又证明了它的逆命题：每个偶完全数均有欧几里得给出的形式. 于是, 偶完全数和 Mersene 素数是相互对应的.

是否存在奇完全数？至今还没有找到一个奇完全数！这个问题已有很多研究, 但仍不知道答案. 关于这个问题的过去进展可见 Guy 的著作 (新版 1994 年), 那里附有一般性参考文献. 下面介绍近来的工作.

试图解决奇完全数问题的方法已有一些固定的模式. 我相信, 讲述这些方法是有益的, 可使读者感受到这个问题为何那么困难. 主要思想是：如果存在奇完全数 N, 对于 N 的不同素因子个数 $\omega(N)$,N 的大小、 N 的积性和加性表达式等可以有什么推论. 现在对于 N 的每种性质作一个综述.

(1) 不同素因子个数 $\omega(N)$.

Hagis(1980, 宣布于 1975) 证明了 $\omega(N) \geqslant 8$.Chein(1979) 在博士论文中也给出同样结果. 1983 年, Hagis 和 Kishore 各自独立地证明了: 若 $3 \nmid N$, 则 $\omega(N) \geqslant 11$.

Dickson 于 1913 年在这个方向得到另一个结果: 对每个 $k \geqslant 1$, 至多有有限个奇完全数 N 使得 $\omega(N) = k$.1949 年 Shapiro 给出一个更简单的证明.

Kanold 在 1956 年将 Dickson 定理推广为研究哪些 N 满足 $\sigma(N)\ /N = \alpha$, 其中 α 是固定的有理数, 而 $\sigma(N)$ 表示 N 的所有正因子之和. 证明需要利用以下事实: 方程 $aX^3 - bY^3 = c$ 至多有有限多个整数解 (X, Y). 利用 Baker 著名的线性型对数方法, Pomerance 在 1977 年对上面不定方程的解数可以得到有效的估计. 取 $\alpha = 2$, 对每个 $k \geqslant 1$ 他证明了: 若奇完全数 N 有 k 个不同的素因子, 则

$$N < (4k)^{(4k)^{2^{k^2}}}$$

1994 年 Heath-Brown 将此结果作了重大改进: 若奇完全数 N 有 k 个不同的素因子, 则

$$N < 4^{4^k}$$

Cook(1999) 又把此结果最下面的 4 改进成 $195^{1/7} = 2.123\cdots$

(2) N 的下界.

Brent,Cohen 和 te Riele(1991) 证明了: 对每个奇完全数 N,$N > 10^{300}$. 在此之前 Brent,Cohen (1989) 和 Hagis(1973) 分别证明了 $N > 10^{160}$ 和 $N > 10^{50}$.Buxton 和 Elmore 在 1976 年宣布 $N > 10^{200}$, 但是证明细节不够清楚, 未被接受. Grytczuk 和 Wojtowicz 在 1999 年对 N 给出更大的下界, 但是 F.Saidak 发现了证明中的

一个问题，作者在 2000 年已知道此事.

(3) N 和乘性结构.

欧拉给出第一个结果： $N=p^e k^2$, 其中 p 为素数， $p \nmid k$, 并且 $p \equiv e \equiv 1 \pmod 4$. 关于 k 的类型也有许多研究结果. 例如，Hagis 和 McDaniel 于 1971 年证明了 k 不是立方数.

(4) N 的最大素因子.

Hagis 和 Cohen 于 1998 年证明了 N 一定有大于 10^6 的素因子. Hagis 和 McDaniel 在早些时候 (1975 年) 证明了 N 的最大素因子一定大于 100110.Muskat 在 1966 年证明了 N 必有大于 10^{12} 的素数方幂的因子.

(5) N 的其他素因子.

1975 年 Pomerance 证明了 N 的第二个最大素因子至少为 139. Hagis(1981) 和 Iannucci(1991) 分别又改进为 10^3 和 10^4. Iannucci 于 2000 年证明了第三个最大素因子超过 100.

Grün 于 1952 年证明了 N 的最小素因子 p_1 满足 $p_1 < \frac{2}{3}\omega(N)+2$.Kishore (1977) 在博士学位论文中对于 $i=2,3,4,5,6$, 证明了 N 的第 i 个最小素因子小于 $2^{2^{i-1}}(\omega(N)-i+1)$.1958 年， Perisastri 证明了

$$\frac{1}{2} < \sum_{p|N} \frac{1}{p} < 2\lg\frac{\pi}{2}$$

这个结果又被 Suryanarayana(1963), Suryanarayana,Hagis(1970) 以及 Cohen(1978) 加以改进.

(6) N 的加性结构.

Touchard 于 1953 年证明了 $N \equiv 1 \pmod{12}$ 或者 $N \equiv 9 \pmod{36}$. Satyanarayana(1959) 对此给了一个简化的证明.

(7) Ore 猜想.

1948 年，Ore 考虑 N 的诸因子的调和均值

$$H(N) = \frac{\tau(N)}{\sum_{d|N}(1/d)}$$

其中 $\tau(N)$ 为 N 的正因子个数. 如果 N 是完全数，则 $H(N)$ 为整数，不论 N 是偶完全数还是奇完全数，这件事都可由欧拉的结果得出. 事实上，Laborde 在 1955 年发现：N 为偶完全数当且仅当

$$N = 2^{H(N)-1}(2^{H(N)} - 1)$$

其中 $H(N)$ 不仅为整数，而且事实上为素数.

Ore 猜想是说：若 N 为奇数，则 $H(N)$ 不能为整数. 所以这个猜想若成立，将推出不存在奇完全数.

当 N 为素数幂或 $N < 10^4$ 时，Ore 证明了他的猜想是正确的. Mills 在 1954 年对于 $N < 10^7$ 和一些特别类型的 N(如 N 的所有素数幂因子都小于 65551^2),Ore 猜想均正确. 这个结果发表于 1972 年.

Pomerance 在一项未发表的工作中证明，当 $\omega(N) \leqslant 2$ 时 Ore 猜想正确. 方法是：若 $\omega(N) \leqslant 2$ 并且 $H(N)$ 为整数，则 N 必为偶完全数. 这是他写信告诉我的.

下面一些结果不区别奇完全数和偶完全数，研究完全数的分布问题. 对每个 $x \geqslant 1$, 定义 $V(x)$ 为不超过 x 的完全数的个数，即

$$V(x) = \#\{\text{完全数 } N \mid N \leqslant x\}$$

极限 $\lim\limits_{x\to\infty}\dfrac{V(x)}{x}$ 表示完全数集合的自然密度. 1954 年, Kanold 证明了 $\lim\limits_{x\to\infty}\dfrac{V(x)}{x}=0$. 所以当 $x\to\infty$ 时, $V(x)$ 的增长速度比 x 慢.

Wirsing(1959) 给出更精细的结果: 存在 x_0 和 $C>0$, 使得当 $x\geqslant x_0$ 时

$$V(x)\leqslant \mathrm{e}^{(C\lg x)/(\lg\lg x)}$$

更早些时候, Hornfeck(1955, 1956),Kanold(1957),Hornfeck 和 Wirsing(1957) 证明了: 对每个 $\varepsilon>0$ 均存在常数 C, 使得 $V(x)<Cx^{\varepsilon}$.

关于奇完全数存在性的上述这些结果是许多人的努力, 其中一些工作相当困难和精细. 我认为这个问题是一个不可征服的堡垒. 如果某人发现了一个奇完全数, 那多半是因为有好的运气. 另一方面, 说奇完全数不存在, 现在也没有任何根据, 需要产生新的思想.

我想用 Sinha(1974) 的一些结果来结束对完全数的介绍, 这些结果很初等, 可看成是轻松的习题 (只需准备好铅笔!): 形为 a^n+b^n $(n\geqslant 2)$ 并且 $\gcd(a,b)=1$ 的偶完全数只有 28 这一个数. 它也是形为 a^n+1 $(n\geqslant 1)$ 的唯一偶完全数. 最后, 没有 $n\geqslant 2$, 使得

$$a^{n^{n^{\cdot^{\cdot^{\cdot^{n}}}}}}+1 \qquad \text{(指数上至少有 2 个 } n\text{)}$$

是偶完全数.

我们曾经将 N 和 $\sigma(N)$ 相比较来刻画完全数. 这里 $\sigma(N)$ 是 N 的所有正因子之和. 如果只要求 $N\mid\sigma(N)$, N 叫作倍完全数. 当 $2N<\sigma(N)$ 时, N 叫作多余的, 而当 $2N\geqslant\sigma(N)$ 时 N 叫作缺欠的. 令 $s(N)=\sigma(N)-N$ 是 N 的小于 N 正因子之和, 我们可以得到一个迭代数列 $s(N),s^2(N),s^3(N),\cdots$ 其中 $s^k(N)=$

$s(s^{k-1}(N))$.Guy 的书中叙述了这个数列的许多有趣的问题．由于篇幅所限，这里不再讨论这些事情.

2.8 拟素数

本节考虑一些合成数，它们具有素数应当具有的每个性质.

2.8A 以 2 为基的拟素数 (psp)

有一个问题通常认为源于古代中国．这个问题是说：如果自然数 n 满足同余式

$$2^n \equiv 2 \pmod n$$

那么 n 是否为素数？

关于这个问题有一些传说和推测，但是抢先发言之前应当谨慎．从人们所相信的古代中国关于数的知识，似乎很难想象这样一个问题居然会提出来．研究数学史的香港大学肖文强给我写信说：

这个神话起源于 J.H.Jeans 在 *Messenger of Mathematics*(1897 年 ~1898 年, 第 27 期) 中的一篇文章. 他写到"在 Thomas Wade 爵士所发现的一篇孔子时代的文章中"包含一个定理：$2^n \equiv 2 \pmod n$ 当且仅当n 为素数．但是在 J.Needham 的巨著《中国的科学与文明》第三卷第 9 章（数学）中驳斥 Jean 的说法，这是把《九章算术》中的一段翻译错了.

这个错误后来又被一些西方学者不断重复，在 Dickson 《数论史》第一卷第 91 页中说，莱布尼茨相信，由这个中国同余式推出 n 为素数是被证明了的．在 Honsberger *Mathematical Gems* 一书第一卷（1973) 题为《一个古老的中国定理和费马》的一章仍在重复这个故事.

这件事现在又找到另一个版本．肖文强于 1992 年来信说：

我刚刚看到一位中国人韩其的博士论文，题目为《康熙年间西方数学的传入和它对中国数学的影响》(1991)，论文研究清代的数学发展．作者对于所谓“古老的中国定理”指出新的证据．根据韩的观点，这个“定理”源于著名数学家李善兰 (1811 ~ 1882)*(所以论述并不古老)*．李把他的这个素数判别法讲给跟他一起翻译西方教科书的合作者 Alexander Wylie．而 Wylie 可能不懂数学便把李的这个判别法写成短文“一个中国定理”，发表在 1869 年香港杂志 *Note and Queries on China* 上．

在后来几个月中，至少有四个读者对李的工作发表了评论．其中一个读者指出李的判别法是错的．其中一位读者是德国人 J.von Gumpach，他后来成为李在北京的同事．有可能 Gumpach 把这个错误告诉给李，因为李善兰后来在关于数论发表的工作目录 (1872 年) 中删去了关于他的判别法的所有文献．但是在 1882 年，清代另一个著名数学家华蘅芳，在关于数的著作中又把李的判别法写了进去，似乎认为它还是对的．这或许能解释为什么中国数学史的西方学者把这个判别法看成是一个古老的中国定理．韩其说，还会发表文章，更仔细论述这个问题．

借此机会，我感谢肖文强提供这些宝贵的信息．关于李善兰的工作读者可参看李岩和杜石然书的英译本 (1987)．

在作了上述历史的评述之后，现在回到同余式 $2^n \equiv 2 \pmod{n}$．它可以称作是“关于拟素数的拟中国同余式”．

这个猜想的第一个反例是 1819 年得到的，比中国的故事要早很多． Sarrus 证明了 $2^{341} \equiv 2 \pmod{341}$，但是 $341 = 11 \times 31$ 为合成数．特别地，费马小定理的逆命题是不对的．具有同样性质的合成数还有 561, 645, 1105, 1387, 1729, 1905 等．

满足同余式 $2^{n-1} \equiv 1 \pmod{n}$ 的合成数 n 叫作拟素数，也叫

作 Poulet 数，因此 Poulet 对这个问题花了不少精力. 特别地，他早在 1926 年就计算了 5×10^7 以内的拟素数，而 1938 年又计算到 10^8(见第四章参考文献).

每个拟素数 n 都是奇数，并且满足同余式 $2^n \equiv 2 \pmod{n}$. 反之，满足 $2^n \equiv 2 \pmod{n}$ 的每个奇合成数 n 也必为拟素数.

每个奇素数 n 也满足上述同余式. 所以若 $2^{n-1} \not\equiv 1 \pmod{n}$, 则 n 一定是合成数. 这可以用来作为素性判定的第一步. 为了对于素数有更多的了解，自然要研究满足 $2^{n-1} \equiv 1 \pmod{n}$ 的那些整数 n.

假如我为《吉尼斯记录大全》写一章关于拟素数的记录，如何组织材料？一些自然的问题基本上和素数情形是一样的. 例如，拟素数有多少？能否告诉我一个给定的数是否是拟素数？是否有产生拟素数的方法？拟素数是如何分布的？

答案不会令人奇怪：拟素数有无穷多个，并且存在许多方法来构作拟素数的无限序列.

Malo 于 1903 年对此给出最简单的证明. 他证明了：若 n 是拟素数，则 $n' = 2^n - 1$ 也是拟素数. 证明是： n' 显然为合成数. 进而若 $n = ab$, 其中 $1 < a, b < n$, 则

$$2^n - 1 = (2^a - 1)(2^{a(b-1)} + 2^{a(b-2)} + \cdots + 2^a + 1)$$

由于 $n \mid 2^{n-1}-1$, 可知 $n \mid 2^n-2 = n'-1$. 于是 $n' = 2^n-1 \mid 2^{n'-1}-1$.

Cipolla 于 1904 年用费马数给出另一个证明：

若 $m > n > \cdots > s > 1$ 为整数， $N = F_m F_n \cdots F_s$ 为费马数乘积，则 N 是拟素数当且仅当 $2^s > m$.

证明 2 模 N 的阶为 2^{m+1}, 而 2 模 $F_m, F_n, \cdots, F_s$ 的阶分别为 $2^{m+1}, 2^{n+1}, \cdots, 2^{s+1}$, 它们的最小公倍数为 2^{m+1}. 所以 $2^{N-1} \equiv 1 \pmod{N}$ 当且仅当 $2^{m+1} \mid N - 1 = F_m F_n \cdots F_s - 1 = 2^{2^s} Q$, 其中

$2 \nmid Q$. 从而给出所需条件 $2^s > m$. □

正如在第一章中指出的，费马数彼此互素，所以上面方法得到彼此互素的拟素数. 由此还可以得到拟素数，它们具有任意多个素因子.

以后还将介绍 Cipolla 给出的生成拟素数的另一个方法.

Lehmer 于 1936 年发现了生成无限多拟素数的一个十分简单的方法，其中每个拟素数都是两个不同素数之积. 方法是：对每个奇数 $k \geqslant 5$, 令 p 是 $2^k - 1$ 的一个本原素因子，而 q 是 $2^k + 1$ 的一个本原素因子，则 pq 为拟素数. 于是对每个 $m \geqslant 1$, 存在至少 m 个拟素数 $n = pq$, 使得

$$n \leqslant (2^{2m+3} - 1)\left(\frac{2^{2m+3} + 1}{3}\right) = \frac{4^{2m+3} - 1}{3}$$

存在着满足同余式 $2^n \equiv 2 \pmod{n}$ 的偶合成数，这可以叫作是偶拟素数. 最小的这种数 $m = 2 \times 73 \times 1103 = 161038$ 是 Lehmer 于 1950 年发现的. Beeger 在 1951 年证明了存在无穷多个偶拟素数，每个偶拟素数至少有两个奇素因子.

拟素数与素数的差别有多大？由 Cipolla 的结果可知，存在拟素数有任意多素因子. 事实上， Erdös 于 1949 年证明了：对每个 $k \geqslant 2$, 存在无穷多拟素数，每个都是 k 个不同素数的乘积.

Lehmer 在 1936 年对于两个或三个不同素因子乘积的情形，给出为拟素数的判别法： p_1p_2 为拟素数当且仅当 2 模 p_2 的阶除尽 $p_1 - 1$, 并且 2 模 p_1 的阶除尽 $p_2 - 1$. 如果 $p_1p_2p_3$ 为拟素数，则 2 模 p_1 的阶和 2 模 p_2 的阶这两个数的最小公倍数除尽 $p_3(p_1 + p_2 - 1) - 1$.

是否存在无穷多整数 $n > 1$, 使得 $2^{n-1} \equiv 1 \pmod{n^2}$ ？这是尚未解决的问题，它等价于下列诸问题当中任何一个 (Rotkiewicz

1965)：

是否存在无穷多个拟素数为完全平方数？

是否存在无穷多个素数 p, 使得 $2^{p-1} \equiv 1 \pmod{p^2}$ ？

这个同余式在研究费马数和 Mersenne 数平方因子时已经见到过. 我在第五章第 5.3 节还要讨论这类素数.

另一方面, 拟素数可以有平方因子. 最小的例子为 $1194649 = 1093^2$, $12327121 = 3511^2$ 和 $3914864773 = 29 \times 113 \times 1093^2$.

2.8B 以 a为基的拟素数 (psp(a))

对每个 $a > 2$ 都可以考虑同余式 $a^{n-1} \equiv 1 \pmod{n}$. 若 n 为素数, 则对每个 $1 < a < n$, 上面同余式均成立. 所以若 $n \geqslant 4, 2^{n-1} \equiv 1 \pmod{n}$ 但是 $3^{n-1} \not\equiv 1 \pmod{n}$, 则 n 不是素数.

这使得人们研究以 a 为基的拟素数 (或叫作 a- 拟素数), 即满足 $n > a$ 和 $a^{n-1} \equiv 1 \pmod{n}$ 的合成数 n.

1904 年, Cipolla 给出构作 a- 拟素数的方法. 设 $a \geqslant 2, p$ 为奇素数并且 $p \nmid a(a^2-1)$. 令

$$n_1 = \frac{a^p - 1}{a - 1}, \qquad n_2 = \frac{a^p + 1}{a + 1}, \qquad n = n_1 n_2$$

则 n_1 和 n_2 是奇数, 而 n 为合成数. 由 $n_1 \equiv n_2 \equiv 1 \pmod{2p}$ 可知 $n \equiv 1 \pmod{2p}$. 由 $a^{2p} \equiv 1 \pmod{n}$ 得到 $a^{n-1} \equiv 1 \pmod{n}$, 于是 n 为 a- 拟素数.

由于存在无穷多素数, 可知对每个 $a \geqslant 2$, 均有无穷多个 a- 拟素数.

文献中有其他办法, 可以很快给出 a- 拟素数的递增序列. 例如 Crocker 在 1962 年给出的方法: 设 a 为偶数, 但是 $a \neq 2^{2^r}$ $(r \geqslant 0)$. 则对每个 $n \geqslant 1, a^{a^n} + 1$ 都是 a- 拟素数. Steuerwald 在 1948 年给出如下方法: 设 n 是 a- 拟素数, 并且 $\gcd(n, a-1) = 1$. 例如, 对

素数 q, 令 $a=q+1$ 而 p 是素数并且 $p>a^2-1$. 像 Cipolla 的构作方法那样，令

$$n_1=\frac{a^p-1}{a-1}\equiv a^{p-1}+a^{p-2}+\cdots+a+1\equiv p \pmod q$$
$$n_2=\frac{a^p+1}{a+1}\equiv a^{p-1}-a^{p-2}+\cdots+a^2-a+1\equiv 1 \pmod q$$

从而 $n=n_1n_2\equiv p \pmod q$. 于是 n 为 a- 拟素数并且 $\gcd(n,a-1)=1$.

现在令 $f(n)=(a^n-1)/(a-1)>n$, 则 $f(n)$ 也是 a- 拟素数. 首先

$$f(n)=\frac{a^{n_1n_2}-1}{a^{n_2}-1}\cdot\frac{a^{n_2}-1}{a-1}$$

为合成数. 进而，由于 n 和 $a-1$ 互素，并且 $a^{n-1}\equiv 1 \pmod n$, 可知 $n\mid(a^n-a)/(a-1)=f(n)-1$, 即 $f(n)\mid a^n-1\mid a^{f(n)-1}-1$, 这证明了 $f(n)$ 是 a- 拟素数. 将这个过程迭代下去，由 $f(n)$ 和 $a-1$ 互素可知

$$\begin{aligned}f(n)&=\frac{[(a-1)+1]^n-1}{a-1}\\&=(a-1)^{n-1}+\binom{n}{1}(a-1)^{n-2}+\cdots+\binom{n}{n-2}(a-1)+n\\&\equiv n \pmod{a-1}\end{aligned}$$

于是 $f(n)$ 为 a- 拟素数，并且 $f(n)$ 和 $a-1$ 互素. 这个过程给出 a- 拟素数的无限递增序列： $n<f(n)<f(f(n))<\cdots$ 其增长情形类似于 $n<a^n<a^{a^n}<\cdots$ 将前面所述的 Lehmer 方法用于 a^k-1 和 a^k+1, 可得到一批 a- 拟素数，每个都是两个不同素数之积.

由这些考虑可知，想找最大的 a- 拟素数是一个没有意义的问题.

Lieuwens 在 1971 年的论文中把 Schinzel 和 Erdös 的关于 2- 拟素数的结果一起加以推广，对每个 $k\geqslant 2$ 和 $a>1$, 都存在无穷

多 a- 拟素数. 每个都恰好是 k 个不同素数的乘积. Rotkiewicz 在 1972 年证明了：对每个素数 p, 如果 $p \nmid a \geqslant 2$, 则存在无穷多 a-拟素数，使得它们均被 p 整除. 对 $p=2$ 的情形， Rotkiewicz 在 1959 年已经证明了这个结果.

有些数可以是对于不同基的拟素数. 例如， 561 是以 2, 5, 7 为基的拟素数. Baillie 和 Wagstaff,Monier 独立地在 1980 年证明了如下结果：

设 n 是合成数，令

$$B_{\mathrm{psp}}(n) = \#\{a \mid 1 < a < n,\ \gcd(a,n)=1,\ n \text{ 为 } a- \text{ 拟素数}\}$$

则

$$B_{\mathrm{psp}}(n) = \left\{\prod_{p|n} \gcd(n-1,\ p-1)\right\} - 1$$

所以若 n 为奇合成数, 并且 n 不是 3 的方幂, 则至少对两个 a, $1 < a \leqslant n-1$,n 是 a- 拟素数.

我们在 2.9 节将会看到，存在合成数 n, 使得对每个 a, $1 < a < n$, $\gcd(n,a)=1$,n 都是 a 拟素数.

表 2.10 取自 Pomerance,Selfridge 和 Wagstaff(1980) 文章，表中对不同的基 (或同时几种基) 给出最小拟素数.

我已经说过，若存在 a, $1 < a < n$, 使得 $a^{n-1} \not\equiv 1 \pmod{n}$, 则 n 为合成数，但反过来不对. 这个方法用来判别某个数为合成数是很有效的. 还有一些类似的同余式，可用来判别某个数为合成数. 我将介绍其中的一些同余式. 这些研究和素性判定问题有密切联系. 事实上，我在 2.3 节和 2.5 节已经不十分明确地讲到这种同余式性质. 在下面将介绍如何由同余式 $a^m \equiv 1 \pmod{n}$ 得到欧拉 a- 拟素数和强 a- 拟素数. 2.10 节讨论 Lucas 拟素数，它们满足 Lucas 序列诸项所满足的同余式.

表 2.10　对于一些基的最小拟素数

基	最小拟素数
2	$341 = 11 \times 31$
3	$91 = 7 \times 13$
5	$217 = 7 \times 31$
7	$25 = 5 \times 5$
2, 3	$1105 = 5 \times 13 \times 17$
2, 5	$561 = 3 \times 11 \times 17$
2, 7	$561 = 3 \times 11 \times 17$
3, 5	$1541 = 23 \times 67$
3, 7	$703 = 19 \times 37$
5, 7	$561 = 3 \times 11 \times 17$
2, 3, 5	$1729 = 7 \times 13 \times 19$
2, 3, 7	$1105 = 5 \times 13 \times 17$
2, 5, 7	$561 = 3 \times 11 \times 17$
3, 5, 7	$29341 = 13 \times 37 \times 61$
2, 3, 5, 7	$29341 = 13 \times 37 \times 61$

2.8C　以 a为基的欧拉拟素数 (epsp(a))

关于勒让德符号的欧拉同余式是说：若 $a \geqslant 2$,p 为奇素数并且 $p \nmid a$, 则

$$\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p}$$

Shanks 于 1962 年由此给出关于以 a 为基的欧拉拟素数 (epsp(a)) 的概念．它们是奇合成数 n, $\gcd(a, n) = 1$, 并且雅可比符号满足同余式

$$\left(\frac{a}{n}\right) \equiv a^{(p-1)/2} \pmod{n}$$

每个 epsp(a) 显然都是 a- 拟素数.

关于 epsp(a) 自然会提出许多问题，现在列举如下：

(e1) 对每个 a, 是否存在无穷多 epsp(a) ?

(e2) 对每个 a, 是否存在 epsp(a), 使得它具有任意多个不同素因子?

(e3) 对每个 $k \geqslant 2$ 和 $a \geqslant 2$, 是否存在无限多 epsp(a), 使得它们都恰好是 k 个不同素因子的乘积?

(e4) 是否存在奇合成数 n, 使得对每个 a, $1 < a < n$, $\gcd(a, n) = 1$, n 都是 epsp(a) ?

(e5) 对每个 n, 有多少 a, $1 < a < n$, $\gcd(a, n) = 1$, 使得 n 是 epsp(a) ?

Kiss, Phong 和 Lieuwens 于 1986 年证明了: 对给定的 $a, k, d \geqslant 2$, 存在无穷多 epsp(a), 它们都是 k 个不同素数之乘积, 并且模 d 同余于 1. 这给出比 (e3)(从而比 (e2), (e1)) 要强的肯定性答案.

Lehmer 于 1976 年证明了: 若 n 是奇合成数, 则不能对每个 a, $1 < a < n$, $\gcd(n, a) = 1$,n 都是 epsp(a). 所以给出 (e4) 否定的答案. 事实上, Solovay 和 Strassen 在 1977 年证明的更多: 对每个合成数 n, 至多有 $\frac{1}{2}\varphi(n)$ 个 a, $1 < a < n$, $\gcd(a, n) = 1$, 使 n 是以 a 为基的欧拉拟素数. 这给出 (e5) 的一个解答. 证明是容易的: 满足 $\left(\frac{a}{n}\right) \equiv a^{(p-1)/2} \pmod{n}$ 的 a 模 n 同余类全体形成 $(\mathbb{Z}/n\mathbb{Z})^{\times}$(模 n 可逆同余类群) 的一个子群. 再由勒让德定理即知此子群至多有 $\frac{1}{2}\varphi(n)$ 个元素.

设 n 为奇合成数. 定义集合

$$B_{\text{epsp}}(n) = \#\{a \mid 1 < a < n,\ \gcd(a, n) = 1,\ n\text{为 epsp}(a)\}$$

Monier 于 1980 年证明了

$$B_{\text{epsp}}(n) = \delta(n) \prod_{p \mid n} \gcd\left(\frac{n-1}{2}, p-1\right) - 1$$

其中

$$\delta(n)=\begin{cases} 2, & v_2(n)-1=\min_{p|n}\{v_2(p-1)\} \\ \dfrac{1}{2}, & \text{有素数 } p \mid n, \text{使得 } 2\nmid v_p(n) \text{ 并且 } v_2(p-1)<v_2(n-1) \\ 1, & \text{其他} \end{cases}$$

而对每个整数 m 和素数 p,$v_p(m)$ 表示 m 的 p-adic 赋值，即满足 $p^{v_p(m)} \mid m$, 但是 $p^{v_p(m)+1} \nmid m$.

2.8D 以 a为基的强拟素数 (spsp(a))

设 n 是奇合成数， $n-1=2^s d,\ 2\nmid d,\ s\geqslant 1$. 令 $1<a<n,\ \gcd(n,a)=1$.n 叫作以 a 为基的强拟素数 (spsp(a)), 是指或者 $a^d\equiv 1 \pmod n$, 或者对某个 $r,\ 0\leqslant r<s,\ a^{2^r d}\equiv -1 \pmod n$.

注意:若 n 为素数,则上述条件对每个 $a(1<a<n,\ \gcd(a,n)=1)$ 都满足.

Selfridge 证明了 (见 Williams1978 年的证明) ：每个 spsp(a) 都是 epsp(a). 反过来则有以下的部分结果.

Malm(1977) 证明：若 $n\equiv 3 \pmod 4$ 并且 n 为 epsp(a), 则 n 为 spsp(a).

Pomerance, Selfridge 和 Wagstaff(1980) 证明：若 n 为奇数，$(a\mid n)=-1$ 并且 n 为 epsp(a), 则 n 为 spsp(a). 特别若 $n\equiv 5 \pmod 8$, n 为 epsp(2), 则 n 为 spsp(2).

关于强拟素数,则有和 2.8C 中欧拉拟素数类似的问题 (s1)~(s5). 1980 年， Pomerance,Selfridge 和 Wagstaff 证明了：对每个 $a>1$, 都有无穷多个 spsp(a), 从而像 (e1) 那样，对于 (s1) 给出肯定的答案. 我在第四章 4.6 节研究拟素数分布时还会介绍更多的结果.

现在我说明对于基为 2 的情形，可以明显地给出无穷多个 spsp (2).

若 n 为 psp(2), 则 2^n-1 也是 spsp(2). 由于有无穷多个 psp(2), 从而明显地给出无穷多个 spsp(2). 这些合成数都是 Mersenne 数. 还容易看出，若一个费马数是合成数，则它为 spsp(2).

类似地，由于存在具有任意多个不同素因子的拟素数，可知 (s2) 和 (e2) 一样，答案也是肯定的. 这是由于：若 $p_1,p_2,\cdots,p_k$ 均除尽拟素数 n, 则 $2^{p_i}-1$ $(1\leqslant i\leqslant k)$ 除尽 spsp(2) 2^n-1.

由于 Selfridge 结果和 Lehmer 关于 (e4) 的否定答案, 可知 (s4) 也有否定的答案. 下面是 Rabin 的一个很重要的定理，它对应于欧拉拟素数的 Solovay 和 Strassen 结果. 我在后面要指出，这个结果和 Monte Carlo 素性试验方法有关系. 利用一点技巧可以证明：

若 $n>4$ 是合成数，则至少有 $3(n-1)/4$ 个 a, $1<a<n$, 使得 n 不是 spsp(a). 所以对每个奇合成数 n, 集合 $\{a\mid 1<a<n,\ \gcd(a,n)=1,\ n$为 spsp$(a)\}$ 至多有 $(n-1)/4$ 个元素. 这给出问题 (s5) 的一个解答.

对于奇合成数 n,Monier(1980) 对于函数

$$B_{\text{spsp}}(n)=\#\{a\mid 1<a<n,\ \gcd(a,n)=1,\ n\ \text{为 spsp}(a)\}$$

给出如下的公式：

$$B_{\text{spsp}}(n)=\left(1+\frac{2^{\omega(n)\nu(n)}-1}{2^{\omega(n)}-1}\right)\left(\prod_{p\mid n}\gcd(n^*,p^*)\right)-1$$

其中

$$\omega(n)\text{为 } n \text{ 的不同素因子个数}$$

$$\nu(n)=\min_{p\mid n}\{v_2(p-1)\}$$

$$v_p(m)\text{为 } m \text{ 的 } p\text{-adic 指数赋值}$$

$$m^*\text{为 } m-1 \text{ 的最大奇因子}$$

最小的 spsp(2) 是 $2047 = 23 \times 89$. 关于对多个基的最小强拟素数是一个有趣和有用的问题，它可用于强素性试验之中.

给了 $k \geqslant 1$, 以 t_k 表示最小整数, 使得 t_k 同时是以 $p_1 = 2, p_2 = 3, \cdots, p_k$ 为基的强拟素数. Pomerance, Selfridge 和 Wagstaff(1980) 和 Jaeschke (1993) 计算出以下数值:

$$t_2 = 1373653 = 829 \times 1657$$

$$t_3 = 25326001 = 2251 \times 11251$$

$$t_4 = 3215031751 = 151 \times 751 \times 28351$$

$$t_5 = 2152302898747 = 6763 \times 10627 \times 29947$$

$$t_6 = 3474749660383 = 1303 \times 16927 \times 157543$$

$$t_7 = t_8 = 341550071728321 = 10670053 \times 32010157$$

表 2.11　25×10^9 以内同时为 spsp(2), spsp(3), spsp(5) 的数

数	psp to base			因子分解
	7	11	13	
25 326 001	no	no	no	2251×11251
161 304 001	no	spsp	no	7333×21997
960 964 321	no	no	no	11717×82013
1 157 839 381	no	no	no	24061×48121
3 215 031 751	spsp	psp	psp	$151 \times 751 \times 28351$
3 697 278 427	no	no	no	30403×121609
5 764 643 587	no	no	spsp	37963×151849
6 770 862 367	no	no	no	41143×164569
14 386 156 093	psp	psp	psp	$397 \times 4357 \times 8317$
15 579 919 981	psp	spsp	no	88261×176521
18 459 366 157	no	no	no	67933×271729
19 887 974 881	psp	no	no	81412×244261
21 276 028 621	no	psp	psp	103141×206281

Jaeschke 还算出：在 10^{12} 以内共有 101 个数同时是以 2, 3, 5 为基的强拟素数. 下面的表 2.11 是数据当中不超过 25×10^9 的那

部分. 我对于表 2.11 再补充上 25×10^9 以内具有平方因子的那些拟素数

$$1194649 = 1093^2$$

$$12327121 = 3511^2$$

$$3914864773 = 29\times113\times1093^2$$

$$5654273717 = 1093^2\times4733$$

$$6523978189 = 43\times127\times1093^2$$

$$22178658685 = 5\times47\times79\times1093^2$$

除了后两个数之外，其余均是强拟素数. 注意上面数中平方因子都是 1093 或 3511 的平方. 我们要在 5.3 节解释这个现象.

2.9 Carmichael 数

Korselt 于 1899 年的一篇短文至今未引起人们的注意，此文考虑更少有的一批数，这批数于 1912 年又由 Carmichael 独立地加以考虑，并且第一个研究这些数的性质. 由于后一篇文章被人们注意，这些数被称作 Carmichael 数. 它定义合成数 n, 并且对每个与 n 互素的 a, $1<a<n$, 均有 $a^{n-1}\equiv1 \pmod n$. 最小 Carmichael 数是 $561=3\times11\times17$.

现在给出 Carmichael 数一个新的刻画. 在 2.2 节定义了函数

$$\lambda(n)=\max_{\substack{1\leqslant a<n\\ \gcd(a,n)=1}}\{a\text{模 } n \text{ 的阶}\}$$

由定义可知 $\lambda(n)\mid\varphi(n)$.Carmichael 证明了: n 为 Carmichael 数当且仅当 n 是合成数并且 $\lambda(n)\mid n-1$(这也相当于: 若素数 $p\mid n$, 则 $p-1\mid n-1$).

由此可知，每个 Carmichael 数都是奇数，并且是大于或等于 3 个不同素数的乘积.

如果 $n = p_1p_2\cdots p_r$ 是 r 个不同素数之积，则 n 为 Carmichael 数当且仅当对每个 $1 \leqslant i \leqslant r$, $p_i - 1 \mid (n/p_i) - 1$. 所以若 n 为 Carmichael 数，则对每个整数 $a \geqslant 1$, 均有 $a^n \equiv a \pmod{n}$.

用 m_a 表示以 a 为基的最小拟素数. Schinzel 在 1959 年注意到：对每个 $a \geqslant 2$, $m_a \leqslant 561$. 并且存在 a 使 $m_a = 561$. 具体说来，设 $p_1, \cdots, p_s$ 是小于 561 的全部奇素数. 对每个 p_i, 由 $p_i^{e_i} < 561 < p_i^{e_i+1}$ 定义整数 e_i. 取 g_i 为模 $p_i^{e_i}$ 的一个原根，由中国剩余定理可求出 a, 使得 $a \equiv 3 \pmod{4}$, $a \equiv g_i \pmod{p_i^{e_i}}$ $(1 \leqslant i \leqslant s)$, 则 $m_a = 561$.

Carmichael 和 Lehmer 决定出下面一些最小的 Carmichael 数：

$561 = 3 \times 11 \times 17$
$1105 = 5 \times 13 \times 17$
$1729 = 7 \times 13 \times 19$
$2465 = 5 \times 17 \times 29$
$2821 = 7 \times 13 \times 31$
$6601 = 7 \times 23 \times 41$
$8911 = 7 \times 19 \times 67$
$10585 = 5 \times 29 \times 73$
$15841 = 7 \times 31 \times 73$
$29341 = 13 \times 37 \times 61$
$41041 = 7 \times 11 \times 13 \times 41$
$46657 = 13 \times 37 \times 97$
$52633 = 7 \times 73 \times 103$
$62745 = 3 \times 5 \times 47 \times 89$
$63973 = 7 \times 13 \times 19 \times 37$
$75361 = 11 \times 13 \times 17 \times 31$
$101101 = 7 \times 11 \times 13 \times 101$
$115921 = 13 \times 37 \times 241$
$126217 = 7 \times 13 \times 19 \times 73$
$162401 = 17 \times 41 \times 233$
$172081 = 7 \times 13 \times 31 \times 61$
$188461 = 7 \times 13 \times 19 \times 109$
$252601 = 41 \times 61 \times 101$

现在考虑彼此有密切联系的以下两个问题：

(1) 是否存在无穷多 Carmichael 数？

(2) 给定 $k \geqslant 3$, 是否有无穷多个 Carmichael 数，它们都恰好为 k 个不同素数的乘积？

第 1 个问题由 Alfrod,Granville 和 Pomerance 于 1992 年解决，答案是肯定的，文章发表于 1994 年. 还可参见 Pomerance 1993 年的综述文章.

人们相信第二个问题的答案也是肯定的，但至今未能解决.

比如说，对于 $k=3$ 的情形都没有解决． Duparc (1952) 在这方面有如下结果 [还可见 Beeger(1950)]：

对每个 $r \geqslant 3$, 只存在有限个 Carmichael 数具有 r 个素因子，并且其中 $r-2$ 个素因子是预先给定的．我在第四章还要回到这些问题．

1939 年， Chernick 给出构作 Carmichael 数的以下方法．设 $m \geqslant 1$ 和

$$M_3(m)=(6m+1)(12m+1)(18m+1)$$

如果右边三个因子都是素数，则 $M_3(m)$ 为 Carmichael 数．由此给出一批具有三个素因子的 Carmichael 数．但是，我们不知道这种数是否有无穷多个．

类似地，若 $k \geqslant 4$, $m \geqslant 1$, 令

$$M_k(m)=(6m+1)(12m+1)\prod_{i=1}^{k-2}(9\times 2^i m+1)$$

如果右边 k 个因子均为素数，并且 $2^{k-4} \mid m$, 则 $M_k(m)$ 是具有 k 个素因子的 Carmichael 数．

用这种方法或者稍加变化的方法，已经得到一些很大的或者具有多个素因子的 Carmichael 数．见 Wagstaff (1980 年 321 位数), Atkin (1980 年 370 位数), Wood 和 Huenemann (1982 年 432 位数), Dubner (1985 年 1057 位数), Dubner (1989 年 3710 位数)．以上例子中的 Carmichael 数都只包含少数几个素因子． Yorinaga (1978) 给出一些 Carmichael 数，其素因子个数多达 15 个．

具有多个素因子的大 Carmichael 数的寻找工作还在继续． Löh 和 Niebuhr 1994 年 (发表于 1996 年) 找到一个 16142049 位的 Carmichael 数，此数有 1101518 个素因子．

记录

目前已知的最大 Carmichael 数是 W.R.Alfrod 和 J.Grantham 于 1998 年得到的，它有 20163700 位，共有 1371497 个素因子. 这个数还有如下性质：对每个 k, $62 \leqslant k \leqslant 1371435$, 此数均被恰有 k 个素因子的某个 Carmichael 数所整除.

基于对这些计算工作的深入理解， Alford,Granville 和 Pomerance 于 1994 年终于证明了一个古老的猜想：存在无穷多个 Carmichael 数.

在 Carmichael 数的计算方面. Pinch 于 1998 年列出 10^{16} 以内这种数的全部清单. 我在第四章 4.6B 节中还要讨论他的发现. 在第四章 4.8 节中要介绍 Carmichael 数的分布.

附录　Knödel 数

对每个 $k \geqslant 1$, 定义集合

$$C_k = \{合成数\, n \mid n > k,\ 并且对每个\ 1 < a < n,\ \gcd(n,a) = 1,\\ 均有 a^{n-k} \equiv 1 \pmod{n}\}$$

则 C_1 就是 Carmichael 数的集合. Knödel 于 1953 年考虑了 $k \geqslant 2$ 的情形. 甚至在证明 Carmichael 数有无穷多个之前， Makowski 于 1962 年就证明了：

对每个 $k \geqslant 2, C_k$ 均是无限集合.

证明　对每个 a, $1 < a < k$, $\gcd(a,k) = 1$, 以 r_a 表示 a 模 k 的阶， $r = \prod r_a$(对满足上述条件的 a 求和), 则 $a^r \equiv 1 \pmod{k}$.

存在无穷多个素数 p, 使得 $p \equiv 1 \pmod{r}$. 这个非常有用定理的证明见第四章 4.4 节. 对每个这种 $p > k$, 记 $p - 1 = hr$. 令 $n = kp$, 则 $n \in C_k$. 这是由于：对于 $1 \leqslant a < n$, $\gcd(a,n) = 1$, 则

$\gcd(a,k)=1$. 于是

$$a^{n-k}=a^{k(p-1)}=a^{khr}\equiv 1 \pmod k$$
$$a^{n-k}=a^{k(p-1)}\equiv 1 \pmod p$$

而 $p \nmid k$, 从而 $a^{n-k}\equiv 1 \pmod n$, 于是 $n=kp\in C_k$. □

由以上证明可知, 当 $k=2$ 时, 对每个素数 $p>3$ 均有 $2p\in C_2$. 这是由 Morrow 于 1951 年证明的.

2.10 Lucas 拟素数

由二项序列 $a^n-1\ (n\geqslant 1)$ 和 Lucas 序列的类比，拟素数自然地可推广成与 Lucas 序列有关的一种数. 对于每个 $a\geqslant 2$, 我们有 a-拟素数及伴随的欧拉拟素数和以 a 为基的强拟素数. 在本节中，对于每个非零整数对 (P,Q) 相应给出 Lucas 拟素数，欧拉 -Lucas 拟素数和强 Lucas 拟素数，它们的用途和拟素数一样.

设 P 和 Q 是非零整数， $D=P^2-4Q$， $(U_n)_{n\geqslant 0}$ 和 $(V_n)_{n\geqslant 0}$ 是其相结合的 Lucas 序列.

在 2.4 节中说过，若 n 是奇素数，则

(10.1) 若 $\gcd(n,D)=1$, 则 $U_{n-(D|n)}\equiv 0 \pmod n$

(10.2) $U_n\equiv (D\mid n) \pmod n$

(10.3) $V_n\equiv P \pmod n$

(10.4) 若 $\gcd(n,D)=1$, 则 $V_{n-(D|n)}\equiv 2Q^{(1-(D|n))/2} \pmod n$

如果 n 是合成数并且同余式 (10.1) 成立，则 n 叫作 (关于参数 (P,Q) 的)Lucas 拟素数，简记为 lpsp(P,Q).

这个定义是没有问题的，但是这种数是否存在？如果存在的话，是否值得去研究它们？

2.10A Fibonacci 拟素数

首先考虑一种有趣的特殊情形，即 $P=1, Q=-1, D=5$ 时的 Fibonacci 数列. 这时， $\mathrm{lpsp}(1,-1)$ 称作是 Fibonacci 拟素数.

最小的 Fibonacci 拟素数是 $323=17\times 19$ 和 $377=13\times 29$. 这是因为 $(5\mid 323)=(5\mid 377)=-1$, 可算出 $U_{324}\equiv 0 \pmod{323}$ 和 $U_{378}\equiv 0 \pmod{377}$.

E.Lehmer 在 1964 年证明了：存在无穷多 Fibonacci 拟素数. 更确切地说，对于每个大于 5 的素数 p, U_{2p} 都是 Fibonacci 拟素数.

Parberry(1970) 和 Yorinaga(1976) 研究了性质 (10.2).Parberry 证明了：若 $\gcd(h,30)=1$ 并且条件 (10.2) 对于 h 成立，则此条件对于 $k=U_h$ 也成立.

进而 $\gcd(k,30)=1$, 并且若 h 是合成数，则 U_h 也是合成数. 这表明：若存在一个 Fibonacci 数 U_n 是合成数，并且$U_n\equiv (5\mid n) \pmod{n}$, 则存在无穷多个这样的数. 不久我将指出，这样的 Fibonacci 数是存在的.

事实上，这也可以由 Parberry 的下述结果推出来：若 p 为素数，并且 $p\equiv 1$ 或者 $4 \pmod{15}$, 则 $n=U_{2p}$ 是奇合成数并且满足性质 (10.1) 和 (10.2). 特别地，存在无穷多个 Fibonacci 拟素数满足 (10.2)(这里我利用了第四章 4.4 节中将要介绍的一个事实：存在无穷多个素数 p, 使得 $p\equiv 1 \pmod{15}$, 对 $p\equiv 4 \pmod{15}$ 也有同样的结果).

如果 $p\not\equiv 1,4 \pmod{15}$, 由 2.4 节中的一些整除和同余性质可知 (10.2) 不成立.

Yorinaga 考虑 Fibonacci 数 U_n 的本原部分. 在 2.4 节讲过，每个 Fibonacci 数 $U_n (n\neq 1,2,6,12)$ 都有本原素因子 p(即 $p\mid U_n$

但是对 n 的每个因子 d, $1 < d < n$, $p \nmid U_d$). 于是 $U_n = U_n^* \times U_n'$, 其中 $\gcd(U_n^*, U_n') = 1$, 并且 $p \mid U_n^*$ 当且仅当 p 是 U_n 的本原素因子. Yorinaga 证明了：若 $m \mid U_n^*$ $(n > 5)$, 则 $U_m \equiv (5 \mid m) \pmod{m}$.

根据 2.4 节中 Schinzel 的结果 (1963), 存在无穷多整数 n, 使得 U_n^* 不是素数. 所以由 Yorinaga 结果可推出存在无穷多奇合成数 n, 使得条件 (10.2) 成立.

Yorinaga 算出 707000 以内所有的 109 个合成数 n, 满足 $U_n \equiv (5 \mid n) \pmod{n}$. 其中某些也是 Fibonacci 拟素数, 比如 $n = 4181 = 37 \times 113$ 和 $5777 = 53 \times 109$ 等, 其中有 4 个是以 2 为基的拟素数，它们为

$$219781 = 271 \times 811$$

$$252601 = 41 \times 61 \times 101$$

$$399001 = 31 \times 61 \times 211$$

$$512461 = 31 \times 61 \times 271$$

Parberry 的另一个结果如下 (后来又被 Baillie 和 Wagstaff 加以推广)：

如果 n 是奇合成数， $5 \nmid n$, 并且 (10.1) 和 (10.2) 成立，则

$$\begin{cases} U_{(n-(5|n))/2} \equiv 0 \pmod{n}, & n \equiv 1 \pmod{4} \\ V_{(n-(5|n))/2} \equiv 0 \pmod{n}, & n \equiv 3 \pmod{4} \end{cases}$$

特别地，由于存在无穷多合成数 n, 使得 $n \equiv 1 \pmod{4}$, 可知有无穷多奇合成数 n 满足 $U_{(n-(5|n))/2} \equiv 0 \pmod{n}$.

对于满足 $V_n \equiv 1 \pmod{n}$ 的合成数 n 也作了研究，其中 $(V_k)_{k \geqslant 0}$ 是 Lucas 数列. 这种数也叫作 Lucas 拟素数，但这里的意义与前不同. 1983 年， Singmaster 发现在 10^5 以内共有以下 25

个合成数是这个意义下的 Lucas 拟素数

$$705, 2465, 2737, 3745, 4181, 5777, 6721,$$
$$10877, 13201, 15251, 24465, 29281, 34561,$$
$$35785, 51841, 54705, 64079, 64681, 67861,$$
$$68251, 75077, 80189, 90061, 96049, 97921$$

2.10B Lucas 拟素数 (lpsp(P,Q))

现在考虑结合任意 (P,Q) 的 lpsp(P,Q). 为了更好地与 a- 拟素数加以对比，我们也沿着同样方式进行讨论，但是此时对每种情形都所知甚少. 例如，对给定的 (P,Q), 我们没有任何一般性算法来得到无穷多个 lpsp(P,Q), 使得每个都是 k 个不同素数的乘积 (除了前述关于 Fibonacci 数之外).

但是，Lieuwens 在 1971 年的论文中证明了：对每个 $k \geqslant 2$ 和给定的 (P,Q), 均存在无穷多个 lpsp (P,Q), 每个都是 k 个不同素数的乘积.

一个奇整数可以是对不同 (P,Q) 的 Lucas 拟素数. 令 $D \equiv 0$ 或 1 (mod 4), 令

$$\begin{aligned} B_{\text{lpsp}}(n,D) = \#\{P \mid 1 \leqslant P \leqslant n,\ \text{存在 } Q,\ \text{使得 } D \\ \equiv P^2 - 4Q \pmod n, n \text{ 为 lpsp}(P,Q)\} \end{aligned}$$

Baillie 和 Wagstaff(1980) 证明了

$$B_{\text{lpsp}}(n,D) = \prod_{p|n}\left\{\gcd\left(n-\left(\frac{D}{n}\right), p-\left(\frac{D}{p}\right)\right)-1\right\}$$

特别若 n 为奇合成数，则有 D 和至少三对不同的 (P,Q), $P^2-4Q=D$, 使得三个 P 模 n 彼此不同，并且 n 为 lpsp(P,Q).

另一个问题为：若 n 是奇数，有多少模 n 不同的 D, 使得存在 (P,Q), $P^2-4Q \equiv D \pmod n$, $P \not\equiv 0 \pmod n$ 并且 n 为

lpsp(P,Q) ？对于 n 是两个不同素数之乘积的情形， Baillie 和 Wagstaff 也讨论了这个问题.

2.10C 欧拉 -Lucas 拟素数 (elpsp(P,Q)) 和强 Lucas 拟素数 (slpsp(P,Q))

给定 P 和 $Q,D=P^2-4Q,n$ 为奇素数. 当 $\gcd(n,QD)=1$ 时，由 2.5 节知

$$\text{(e1)}\qquad \begin{cases} U_{(n-(D|n))/2}\equiv 0 \pmod n, & (Q\mid n)=1\\ V_{(n-(D|n))/2}\equiv D \pmod n, & (Q\mid n)=-1\end{cases}$$

这给出如下的定义：奇合成数 n, $\gcd(n,QD)=1$, 叫作关于 (P,Q) 的欧拉 -Lucas 拟素数，简记为 elpsp(P,Q), 是指它满足条件 (e1).

设 n 是奇合成数， $\gcd(n,D)=1$， $n-(D\mid n)=2^sd$, $s\geqslant 0$, $2\nmid d$. 如果

$$\text{(s1)}\qquad \begin{cases} U_d\equiv 0 \pmod n, & \text{或者}\\ V_{2^rd}\equiv 0 \pmod n, & \text{对每个 } r,\ 0\leqslant r<s\end{cases}$$

则 n 叫作关于 (P,Q) 的强 Lucas 拟素数，简记为 slpsp(P,Q). 这时一定有 $\gcd(n,Q)=1$.

若 n 为奇素数， $\gcd(n,QD)=1$, 则 n 满足上述条件 (e1) 和 (s1). 又若 n 为 elpsp(P,Q) 并且 $\gcd(n,Q)=1$, 则 n 为 lpsp(P,Q).

elpsp(P,Q) 和 slpsp(P,Q) 有何联系？就像欧拉拟素数与以 a 为基的强拟素数之间的关系一样， Baillie 和 Wagstaff 证明了：若 n 为 slpsp(P,Q), 则 n 为 elpsp(P,Q). 这是 Selfridge 结果的一个类比.

反过来，若 n 为 elpsp(P,Q), 并且或者 $(Q\mid n)=1$ 或者 $n-(D\mid n)\equiv 2 \pmod 4$, 则 n 为 slpsp(P,Q), 这是 Malm 结果的一个类比.

如果 $\gcd(n,Q)=1$，n 为 $\mathrm{lpsp}(P,Q)$，$U_n \equiv (D \mid n) \pmod n$ 并且 n 为 $\mathrm{elpsp}(P,Q)$，则 n 也是 $\mathrm{slpsp}(P,Q)$. 对于 Fibonacci 数的特殊情形，如前所说 Parberry 已经证明了此项结果.

前面我曾提到 Lehmer 的一个结果，即不存在奇合成数，它对所有可能的基 a 都是 $\mathrm{epsp}(a)$.Willaims (1977) 对此也给出一个类比结果：给了 $D \equiv 0$ 或 $1 \pmod 4$，若 n 为奇合成数，$\gcd(D,n)=1$，则存在非零整数 P,Q，$P^2-4Q=D$，$\gcd(n,D)=\gcd(n,Q)=1$，使得 n 不为 $\mathrm{elpsp}(P,Q)$.

采用现在的记号，我已经说过 Parberry 对于 Fibonacci 数证明了无穷多个 $\mathrm{elpsp}(1,-1)$.Kiss,Phong 和 Lieuwens(1986) 对此作了改进：给定 (P,Q)，使对应序列 $(U_n)_{n\geqslant 0}$ 是非退化的 (即对每个 $n\geqslant 0$，$U_n\neq 0$)，又给了 $k\geqslant 2$，则存在无穷多个 $\mathrm{elpsp}(P,Q)$，每个都是 k 个不同素数的乘积. 并且若又给定 $d\geqslant 2$，而 $D=P^2-4Q>0$，则 k 个素因子都可取为形式 $dm+1$ $(m\geqslant 1)$.

像 Fibonacci 数一样，作者现在同时考虑同余式 (10.2) 和 (10.3)、(10.4) 式. 可以证明：若 $\gcd(n,2PQD)=1$，并且 n 满足 (10.1)~(10.4) 当中任意两个，它必满足另外两个条件.

1986 年，Kiss,Phong 和 Lieuwens 把 Rotkiewicz(1973) 的一个结果推广为：给了 $P,Q=\pm 1$ 但是 $(P,Q)\neq(1,1)$,$k\geqslant 2$ 和 $d\geqslant 2$，则存在无穷多整数 n,n 是以 2 为基的欧拉拟素数，满足同余式 (10.1)~(10.4)，并且是 k 个形如 $dm+1$ $(m\geqslant 1)$ 的素数的乘积.

2.10D Carmichael-Lucas 数

沿从拟素数到 Carmichael 数的同样思考线索，自然地考虑如下的数. 给了 $D\equiv 0$ 或 $1 \pmod 4$，整数 n 叫作 (结合于 D 的)Carmichael-Lucas 数，是指 $\gcd(n,D)=1$，并且对非零互素的 (P,Q)，$P^2-4Q=D$，$\gcd(n,Q)=1$,n 均为 $\mathrm{lpsp}(P,Q)$.

这种数是否存在？开始时这并不清楚. 当然，若 n 是结合 $D=1$ 的 Cramichael-Lucas 数，则 n 为 Carmichael 数. Williams 于 1977 年证明了：

如果 n 是结合于 $D=5$ 的 Carmichael-Lucas 数，则 n 是 $k \geqslant 2$ 个不同素数 p_i 的乘积，并且 $p_i-(D \mid p_i)$ 整除 $n-(D \mid n)$ $(1 \leqslant i \leqslant k)$.

注意 $323 = 17 \times 19$ 是 Carmichael-Lucas 数 $(D=5)$, 但不能是 Carmichael 数，因为它只是两个素数的乘积.

将 Chernick 方法加以修改，可以产生许多 Carmichael-Lucas 数，如 $1649339 = 67 \times 103 \times 239$ 是这种数 (对于 $D=8$).

2.11 素性检测和因子分解

我在这最后一节里处理一个热门话题，充满新奇的思想，作了大量的研究，并且又有直接的应用.

数论有直接应用！在四十年前谁会有这种梦想？不是我，也不是一些别人，是冯. 诺依曼 (Von Neumann). 可怜的数论，这位受人敬畏的数学皇后被贬为 (也许是升为？) 作坊里的仆人.

近年来，素性检测和因子分解问题有了快速进展，采用了越来越多的数论深刻结果. 聪明的头脑设计出灵巧的算法程序，同样聪明的技术师发明了技巧，使程序于合理的时间内在工程上得以实现，这就产生数论的一个全新的分支 —— 计算数论.

在本章的前几节中，我试图提供素性检测一些主要算法程序所需要的基础理论. 但是这还不够，因为素性检测近年来的发展还采用了雅可比和、代数数论、椭圆曲线、阿贝尔簇等很多高深的数论，这些已远远超出本书的范围. 对此有兴趣的读者需要阅读一些补充读物. 目前这方面已有许多好的综述文章和书籍，我将

在适当的地方向大家作一些推荐.

尽管有上述的不足之处，我感到在这里介绍一下素性检测和因子分解还是有益的. 在介绍中可能有不完备之处，也请大家原谅.

首先是经济上的问题：做一件事的花费有多大？然后我用较大篇幅介绍素性检测, 讲述近来提出的某些因子分解方法, 最后简单地谈一下它们在公钥密码学上的应用. 如果这些介绍使读者有兴趣, 我会感到很高兴, 并且想推荐读者进一步去看 Williams(1998) 和 Crandall 与 Pomerance(2001) 的书.

2.11A 检测的成本

实现关于数 N 的一个算法所需的成本是和所用时间成正比的，从而依赖于所用的机器、程序以及数 N 的大小.

各种运算需要以适当的方式加以考虑，因为大数的加法和乘法比小数运算要多花时间. 所以在最后的分析中，成本和在数字诸位上的运算个数成正比. 在运算时，输入不是整数 N, 而是 N 的 b 进制展开的诸位数字，这些数字的个数是与 $\lg N$ 成正比的.

一个算法叫作多项式算法，是指存在一个多项式 $f(X)$, 使得对每个数 N, 对于 N 实现这个算法所需时间不超过 $f(\lg N)$. 若一个算法不是多项式算法并且对每个 N, 用这个算法计算 N 的时间以 $f(N)$ 为上界，这个算法叫指数型算法，这是由于 $N = \mathrm{e}^{\lg N}$. 多项式算法被认为是经济实用的.

算法复杂性理论专门研究如何决定算法所需时间的各种界. 这是一项很麻烦的工作，需要对所用方法进行仔细的分析. 通过发明一些聪明的技巧，有时可以把算法简化成只需多项式时间的新算法.

可以说，素性检测 (以及许多其他问题) 都面临以下主要挑

战：

是否存在实现检测的多项式算法？

对于素性检测，这个挑战恰好在不久前被肯定地加以解决，我在适当的地方将作进一步说明．但是在这之前，我首先介绍不是多项式算法的一些素性检测方法，这些方法在实际中是很有效的．

如果已知 N 是合成数， $N=ab$, 证明只需要一个运算，即做乘法 $a\cdot b$, 验证它是否为 N. 在位运算所花时间不超过 $(\lg N)^2$. 这是在发现 a 和 b 之后的算法，而发现 a 和 b 则需要"超人的洞察力" (Lenstra 的语言), 或者像 Cole 把 Mersenne 数 M_{67} 分解成

$$M_{67}=2^{67}-1=193707721\times 761838257287$$

花了三年当中的所有星期日．如果已知 p 为素数，需要多少次运算来证明这件事？答案并不容易． Pratt 于 1975 年证明了只用 $C(\lg p)^4$ 个位上的运算即可, 其中 C 是一个正的常数． Pomerance 在 1987 年用定义在模 n 整数上椭圆曲线点数的 Hasse-Weil 界，证明在已知 p 为素数的情况下，验证 p 的素性只需 $C\lg p$ 个模 p 乘法运算．这比所有以前的验证方法都好．

我们这里的问题与上面的讨论完全不同，我们是在不知 N 为素数或合成数的情况下判定 N 的素性．

2.11B 素性检测的一些方法

目前有许多种素性检测方法．按照不同的观点，这些方法可以分类为

$$\begin{cases}\text{对某些特殊形式数的素性检测}\\ \text{对任意正整数的素性检测}\end{cases}$$

或者

$$\begin{cases}\text{完全绝对的检测}\\ \text{基于某些猜想的检测}\end{cases}$$

或者

$$\begin{cases}\text{确定型的检测}\\ \text{概率型或叫蒙特·卡罗 (Monto Carlo) 检测}\end{cases}$$

我将依次考虑上述各种素性检测方法.

如果 $N-1$ 或者 $N+1$ 有足够多的素因子已经知道，则 2.3 和 2.5 节中所述方法是多项式算法. 这就是特殊情况的素性检测，它们对具有特殊形式的数是很有效的. 相比之下，一般情况下的素性检测可用于任何数，并不是为了使得对任何一类数专门设计得更为有效.

素性检测的正确性评判是基于数论，但是有些检测评判需要采用没有被证明的某些猜想，如黎曼猜想的某种形式.

有许多检测是确定型的，即检测步骤是事先安排好的. 而另一些检测在过程中的某些步骤可以随机选择.

如果对 N 进行素数检测，希望输出是下列两个答案之一："N 是素数"或者"N 是合成数". 可有些检测的输出为"N 是合成数"或者"N 具有素数的某个性质". 由于每次检测都是以某种概率来判定 N 的素性，这类检测叫作概率型或蒙特·卡罗型检测.

如果检测表明数 N 以很高的概率为素数，通常把 N 叫作是一个概率素数. 当然，每个整数 $N>1$ 或者是素数，或者是合成数. 所谓"概率素数"不过是表明目前还缺乏足够的知识来判定它到底是素数还是合成数.

如果经过一次检测表明 N 为素数，检测通常要做大量的计算，可能会发生人为或机器的错误，所以非常重要的事情是验证

所得的结论. 两次或三次重复检测, 但是最好是采用另外的算法程序或采用另外的机器, 如果得到同样的输出结果, 则足以相信其结果的正确性, 但这仍不是证明.

由上述可知, 一个数在检测中被宣布是素数, 非常希望能保证它的素性. 这种保证应当是一个数学证明. 现在我就介绍几个(只是目前所用方法中的少数几个) 素性检测方法.

试除法

对于任意正整数 $N > 1$, 决定 N 的素性的最天真的方法是用所有不超过 $\sqrt{N}$ 的素数去除 N. 我们在第四章中会知道, 当 N 很大时, 不超过 $\sqrt{N}$ 的素数大约有 $2\sqrt{N}/\lg N$ 个 (以后会说得更精确). 所以要进行 $2\sqrt{N}/\lg N$ 次运算 (其中 $C > 0$ 是常数), 于是所用时间为 $2\sqrt{N}/\lg N$. 这不是多项式算法.

Miller 检测

Miller 于 1976 年提出一种素性检测方法, 其证明要用到黎曼猜想的一个推广形式. 我在这里不解释这个猜想的确切含义, 但是在第四章 4.1 节中要讨论经典的黎曼猜想本身.

为叙述 Miller 检测, 需要定义强拟素数的那些同余式. 但是我们采用 Robin 建议的更方便的术语.

设 N 为整数, $N-1=2^sd$, 其中 $s \geqslant 0$ 而 d 为奇数. 对于 $1<a<N$, $\gcd(a,N)=1$, 我们称 a 是 N 的一个证据, 是指 $a^d \not\equiv 1 \pmod{N}$, 但是对每个 r, $0 \leqslant r < s$, 均有 $a^{2^r d} \not\equiv -1 \pmod{N}$.

如果 N 有一个证据, 则 N 是合成数. 若 N 为合成数, 并且对某个 a, $1<a<N$, $\gcd(a,N)=1$, a 不是 N 的证据, 则 N 为 $\mathrm{spsp}(a)$. 反过来, 若 N 为奇数并且是 $\mathrm{spsp}(a)$, 则 a 不是 N 的证据.

采用这种术语，为了证明 N 是素数，只需证明每个 a，$1 < a < N$，$\gcd(a, N) = 1$ 都不是 N 的证据．当 N 很大时，这项任务是非常繁重的．所以想到只对某些较小的 a 来检查它们是否为 N 的证据．在这里需要利用广义黎曼猜想，由此可证明

Miller 检测 *若 N 是奇数．如果存在某个 a，$1 < a < 2(\lg N)^2$，$\gcd(a, N) = 1$，使得 a 为 N 的证据，则 N 为合成数，否则 N 为素数．*

根据 2.8 节中报告的计算结果，在 25×10^9 以内对于基 $2, 3, 5, 7$ 同时为强拟素数的只有一个数 3215031751．所以若 $N < 25 \times 10^9$ 并且 N 不是这个数，而且 $2, 3, 5, 7$ 不是 N 的证据，则 N 为素数．Jaeschke(1993) 证明了这件事对于 $N < 118670087467$ 均对．

这个检测用袖珍计算器就可进行．

检测一个数 a 是否为 N 的证据，需要的运算次数为 $C(\lg N)^5$，其中 C 是正的常数．所以在广义黎曼猜想成立的假定之下，这是多项式算法．

Lenstra 于 1979 年发表了对 Miller 方法的一个更有效的改进方案，并在 1982 年再次讨论这个检测．还可参见 Wagon(1986) 的综述文章．

APR 检测

Adleman,Pomerance 和 Rumely(1983) 给出的素性检测方法通常称为 APR 方法，是这方面的一个突破．它的特点有：

(i) 这是确定型的一般性检测，所以可用于任意自然数 N，不需要 $N - 1$ 或 $N + 1$ 的任何因子分解知识．

(ii) 计算量 $t(N)$ 几乎是多项式型的．更确切地说，存在有效

可计算的常数 $0 < C' < C$, 使得

$$(\lg N)^{C' \lg\lg\lg N} \leqslant t(N) \leqslant (\lg N)^{C \lg\lg\lg N}$$

(iii) 检测结果的正确性有严格的数学证明. 并且在这个领域中第一次采用了代数数论中高深的结果. 检测中使用单位根和关于幂剩余符号的一般互反律 (我不能解释这些概念, 因为它们大大超出了本书的范围).

一直到 2002 年, APR 检测在所有确定型一般性素性检测中都是计算量最小的方法. 在这个方法提出后不久, Cohen 和 Lenstra (1984) 对 APR 方法加以改进, 使之更加灵活, 在证明中用雅可比和代替互反律, 并且为实际应用提供了新的检测程序. 从而第一次可以检测 200 位以内的数 N, 只需 10 分钟左右的时间, 而 100 位的 N 只需 45 秒钟.

1987 年, Cohen 和另一个 Lenstra(哥哥) 用 15 分钟完成了对 247 位数 $2^{892}+1$ 的素性判定.

Lenstar 在 Bourbaki 讨论班 (Exposé 576 1981) 上介绍了 APR 检测方法. 还可参见 Lenstra(1982), Nicolas(1984) 或 Cohen(1993) 的重要著作.

椭圆曲线检测

Atkin 于 1986 年给出他自己的一种新检测方法, 首次使用有限域上的椭圆曲线. 它是多项式型的概率算法, 具有严格的证明. 如果输出为“素数”, 则给出一批数来, 然后由这批数可容易验证 N 确实为素数, 不需要重复原来的计算. 这批数叫作 N 的“证书”.

Atkin 和 Morain(1993) 发表一篇长文介绍他们的方法“椭圆曲线素性证明 (ECPP) ”, 描述了方法的各种特点. 这个算法由

Morain 加以改进，从而证明和确认了许多 1000 位以上的有趣整数是素数．而且检测采用了很有效的装置，至今仍在使用．

这个检测方法介绍起来相当困难，我甚至在这里也不能说明 ECPP 算法的基本步骤．

记录

由一般性素性检测方法得到的最大素数是 5878 位的 16282536 $\cdots$ 36478311．这个素数的证书由 J.L. Gómez Pardo 于 2003 年 2 月得到，采用 M.Martin 的 ECPP 硬件设备，在一个最快的 PC 机上计算了 3581 小时 (大约 21 个星期)．证书的 text 文件中有将近 5800000 个字符 (请读者想象一下这需要多少本书把它打印出来)．使用目前的证书，这个数在两天之内即可认证为素数．

为了说明 ECPP 方法在过去几年里所取得的超常成绩，我在这里列出前人的一些记录：

素数	位数	时间
$10^{5019}+(3^2\times 7^5\times 11^{11})$	5020	2001 年 9 月
$10^{3999}+4771$	4000	2001 年 5 月
$(348^{1223}-1)/347$	3106	2001 年 1 月
$(30^{1789}-1)/29$	2642	2000 年 10 月
$(2^{7331}-1)/458072843161$	2196	1997 年 10 月

前 4 个记录都是 La Barbera 兄弟和 Martin 的工作．最后一个素数是 Mersenne 数

$$M_{7331}=458072843161\times P2196$$

的素因子，由 E.Mayer 和 F.Morain 用 Morain 的 ECPP 程序验证它的素性．

为了感受一下一个一般性的素性检测方法效果如何，一个好的想法是将此法用于随机数，比如每位数字用有 10 个位置的轮子转出来．有些自然产生的数 (如圆周率 π) 的小数部分数字像是随机分布的．

1999 年 9 月， Y.Kanada 和同仁计算了 π 的 206×10^9 位数字．统计分析表明每位数字都像是随机的．特别地， Caldwell 和 Dubner(2000) 对于 π 的每段是否为素数，其频率和随机性颇为一致． 2002 年 12 月 Kanada 宣布他计算了 π 的 1.2411×10^{12} 位，详见 Bailey(2003)．这让我想起一个不能忘怀的故事． Ludolph van Ceulen 由于正确地计算了 π 的 35 位数字 (他去世后于 1615 年发表) 而闻名于世．这些数字刻在他的墓碑上．我祝愿 Kanada 活得长久，把他的 π 值刻在墓碑上会造成麻烦．

蒙特 · 卡罗方法

20 世纪初,坐落在蒙特 · 卡罗城 (Mattia Carlo) 的赌场 (casino) 吸引了沉迷于赌博的君主和冒险家们，悲剧和运气均由旋转的轮盘所主宰．

我曾经兴致勃勃地读过 Luigi Pirandello 的一本小说，讲述巴斯卡在蒙特 · 卡罗和在他自己的西西里乡村，运气如何关照他并改变了他的生活．但是蒙特 · 卡罗城并不总是好的去处，更常见的代价是完全破产甚至自杀！如果你进行蒙特 · 卡罗素性检测并且不成功的话，我衷心地希望你千万不要有自杀的念头．

共有三种蒙特 · 卡罗素性检测．分别由 Baillie 和 Wagstaff (1980), Solovay 和 Strassen (1977) 以及 Rabin(1976, 1980) 提出来的．在每个检测中使用一些证书 a, 它们是类似于数 psp(a), epsp (a), spsp(a) 所满足的那些同余式．这里我想简单介绍一下 Rabin 检测．

Rabin 的检测与 Miller 检测很类似. 基于 Solovay 和 Strassen 的同样思想， Rabin 提出如下检测方法:

第 1 步: 随机地取 k (>1) 的小整数 a, $1 < a < N$, $\gcd(a, N) = 1$.

第 2 步: 对这些 a 依次检测 N 是否满足以 a 为基的强拟素数定义条件. 即把 N 表示成 $N-1=2^s d$, 其中 $s \geqslant 0$, $2 \nmid d$, 计算是否 $a^d \equiv 1 \pmod N$ 或者 $a^{2^r d} \equiv -1 \pmod N$(对每个 r,$0 \leqslant r < s$) 成立.

如果发现某个 a, 使上述条件不成立, 则 N 为合成数. 否则在 N 是素数时, 上面检测判定 N 为素数的概率大于等于 $1-1/4^k$. 所以对于 $k=30$, 在 10^{18} 次检测中至多判错一次.

如果你想把一批素数卖给公钥密码体制的用户 (我很快就要介绍素性检测和大数分解在密码学中的应用) , 并且你确信或者极大程度上确信你卖的是素数, 你可以在广告词中写上“保证满意, 否则照价赔偿”. 利用 Rabin 检测, 你可以放心地发展买卖, 产品一定会有好的信誉.

近来的 AKS 检测

2002 年 8 月， Agrawal,Kayal 和 Saxena 在网页上发表文章, 介绍一个一般性、确定型和完全证明的素性检测多项式算法. 这就对我在本节开始所提出的那个长期未解决的问题给出肯定性的答案.

这个检测的理论基础是一个命题, 除了其中一步之外, 这个命题只涉及系数是模 N 整数的一些简单的多项式和一个二项式. 而其中关键一步 (至少在目前还需要这一步) 是 Fouvry 在筛法理论中的一个深刻的定理. 我想叙述一下这个定理 (原始形式比它还要强):

令 $\theta = 0.6687\cdots > 2/3$. 对每个 $x > 2$, 均存在素数 p ($x^\theta < p < x$) 和 k(k 不为 3 的方幂) 使得 $2kp+1 \leqslant x$ 并且 $2kp+1$ 为素数.

将这个检测加以修改, 有理由希望使检测不依赖于 Fouvry 这样深刻的定理.

采用快速乘法, 这个检测所需时间开始时的估计为 $(\lg N)^{12}$, 后来降为 $(\lg N)^{7.5}$. 关于复杂性的分析还可见 Morain 文章 (2002).

我请 Agrawal 提供 AKS 算法的简短说明. 感谢他的合作, 下面是他所写的说明.

新的素性检测算法的中心思想是刻画素数的下列恒等式:

N 为素数当且仅当 $(1-X)^N \equiv 1 - X^N \pmod N$

验证此恒等式的最简单有效方法是随机地选取一个小次数多项式 $Q(X)$, 然后模 $Q(X)$ 检查这个恒等式. 结果以很高的概率是正确的, 由此得到一个十分简单的多项式概率算法.

为了得到确定型算法, 一种方法是要证明: 如果恒等式不成立, 则只需模 "少数" 很小次数的多项式 $Q(X)$, 检查就会失败, 最简单方法是取一些 $Q(X) = X^r - 1$, 其中 r 较小.

以下用 $P_1(X) \equiv P_2(X) \pmod{X^r-1,\ n}$ 表示 $P_1(X)$ 和 $P_2(X)$ 用 $X^r - 1$ 除的两个余式的系数模 n 是相等的. 则可以证明

$N = p^k$(p 为素数) 当且仅当对于 "少数" a 和 r, 均有 $(a - X)^N \equiv a - X^N \pmod{X^r - 1,\ p}$

这个结果比前述命题要弱. 事实上, 还可固定一个值 r. 由这个刻画可直接得到一个确定型有效的素性检测方法, 模 N 检测这个恒等式 (而不是模 p), 方法的最后形式可用于 N 为素数幂情形.

上述等价的一个方向容易证明, 另一个方向的证明要用下列

诸事实：

(i) 若对一些 a 有 $(a-X)^N \equiv a-X^N \pmod{X^r-1,\ p}$，对于由这些一次多项式 $(a-X)$ 生成的乘法群中的任何多项式 $g(X)$，均有

$$g(X)^N \equiv g(X^N) \pmod{X^r-1,\ p}$$

由此得到指数数量级的一些多项式 $g(X)$，使上述恒等式成立，只要 p 模 r 的阶比较大，这一点用筛法理论的已知结果是可以做到的.

(ii) 若上式 $g(X)^N \equiv g(X^N) \pmod{X^r-1,\ p}$ 成立，并且显然有 $g(X)^p \equiv g(X^p) \pmod{X^r-1,\ p}$，可知对任何 $s=n^i p^j$

$$g(X)^s \equiv g(X^s) \pmod{X^r-1,\ p}$$

(iii) 由于 X 的方幂可模 X^r-1 约化，从而存在 s,t $(s \neq t)$，使得

$$g(X)^s \equiv g(X^t) \pmod{X^r-1,\ p}$$

如前所述，利用筛法中的已知结果可以保证，当 s 和 t 均小于 (i) 中群的体积时，上面恒等式不可能成立.

2.11C 超大素数和奇妙素数

Yates 在 1983 和 1984 文章中把超过 1000 位的素数称之为“超大 (titanic) 素数”. 在题为“巨人的沉落”的这篇文章中，Yates 列出已知最大素数的一个清单. 到 1985 年 1 月 1 日，他知道 581 个超大素数，其中有 170 个超过 2000 位. 这些素数都写在文章中. 1988 年 9 月，Yates 的清单已经包含了 876 个超大素数. 一个六人小组 (J.Brown,L.C.Noll,B.Parady,G.Smith,J.Smith 和 S.Zarantonello) 于 1990 年初宣布发现了 550 个新的超大素数.

这些素数均有特殊形式，一些为 Mersenne 素数，另一些有形式 $k \times 2^n \pm 1$ 或者 $k \times b^n + 1$ $(b > 2)$, 因为对这类数存在更有效的素性检测算法.

1992 年，Yates 又把超过 10000 位的素数叫作"超霸 (gigantic) 素数". 对于多于 1000000 位的素数，我们叫作"百万位级素数" (megaprimes). 我已经说过，目前所知的最大 Mersenne 素数是百万位级素数. 在 Yates 去世之后， C.Caldwell 成为超大素数、超霸素数和其他珍宝的收藏者，他也是"素数秘闻"这一信息丰富而快捷的互联网作者和管家. 我从这个网站获益匪浅，比对圣地亚哥动物园的兴趣还大.

由于素数检测的飞速进步，素数清单几乎每天都在增大. 到 2002 年底，超过 30000 位的素数已经知道了 5000 个 (只有一部分在 Caldwell 清单之中). 要列出这些数是徒劳的，因为我清楚的知道，这些目前已知的超大素数、超霸素数和百万级素数已经超过了本书的总行数. 但是我想向大家展示一些奇妙的素数.

回文 (palindromic) 数 (以 10 为基) 是十进制表示为 $N = a_1a_2\cdots\ a_n$ 的整数，其中诸位数字 a_i $(0 \leqslant a_i \leqslant 9)$ 满足 $a_1 = a_n$, $a_2 = a_{n-1}, \cdots$ 一些古老的神秘传说常常和各种数有关 (完全数、亲和数、过剩数等), 所以回文数至今还受到算命学家的注意.

Dubner 花了许多年找到越来越大的回文素数. 他的最高记录一直保持到 2001 年，即保持到他发现 39027 位的素数 $10^{39026} + 4538354 \times 10^{19510} + 1$.

记录

目前所知最大回文素数是 104281 位的 $10^{104281} - 10^{52140} - 1$, 由 D.Heuer 于 2003 年 1 月发现, 使用了名为 PrimeForm 的软件, 软件发明人有 C.Nash, Y.Gallot 和 G.Woltman.

在此之前的记录有 Dubner 的三重回文素数 $10^{35352}+2049402\times 10^{17673}+1$，它有 35353 位. 35353 也是回文素数，共有 5 位. 而 5 也是回文素数！

我们还可以考虑看起来令人头痛的问题：给定 $k\geqslant 4$，求一个序列 $N_1,N_2,\cdots,N_k$，使得每个 N_i 都是回文素数，并且对每个 $i=1,\cdots,k-1,N_{i+1}$ 是 N_i 的位数.

为了描述后面的珍宝，我采用以下记号：如 $(23)_4$ 表示23232323，而 $(1)_{15}$ 表示连续 15 个 1 等.

记录

(1) 所有数字均属于 (2,3,5,7) 的最大已知素数是

$$
\begin{aligned}
&72323252323272325252\times\frac{10^{3120}-1}{10^{20}-1}+1\\
=&(72323252323272325252)_{156}+1
\end{aligned}
$$

它是 Dubner 于 1992 年发现的，共 3120 位.

(2) 所有数字为 0 或 1 的最大已知素数为 $1(0)_{15397}1110111(0)_{15397}1$，共 30803 位，它也是回文素数，由 Dubner 于 1999 年发现.

(3) 形如 $d(9)_n$(其中 $3\nmid d$) 的最大已知素数为

d	n	发现时间 (年)
1	55347	2002
2	49314	2002
4	21456	2001
5	34936	2001
7	49808	2002
8	48051	2000

其中多数由 E.J.Sorensen 发现，最后一个由 Dubner 发现，他们都采用了 Gallot 算法.

(4) 所有数字均为奇数的最大已知素数为 $1(9)_{55347}$，即上表中的第一个数.

(5) G.Löh 和 Y.Gallot 于 2000 年发现的素数 $105994\times10^{105994}+1$ 是目前已知的最大素数，其中数字为 0 的个数最多.

(6) 最奇妙的素数是

$$(1)_{1000}(2)_{1000}(3)_{1000}(4)_{1000}(5)_{1000}(6)_{1000}(7)_{1000}(8)_{1000}(9)_{1000}(0)_{6645}1$$

它有 15646 位，由 Dubner 于 2000 年发现.

(7) 最后，1000 位的素数中最小者为 $10^{999}+7$，由 P.Mihăilescu 于 1998 年证明了它是素数.

2.11D 因子分解

大数分解是一个困难问题：目前没有多项式算法. 它也是一个重要的问题，在公钥密码体制中有名声大振的应用.

可是我不想在这里讨论因子分解方法，因为这又会离本书的对象 (素数的记录) 太远. 我想最好是介绍一些书籍和研究性论文. 现在按时间顺序介绍一些书籍.

Brillhart,Lehmer,Selfridge,Tuckerman 和 Wagstaff(1983) 书中包含 $b^n\pm1$ $(b=2,3,5,6,7,10,11,12)$ 对于 n 的各种范围的因子表. 其中给出 $n<1200$ 范围内 2^n-1 的因子. 对较大的基 b，n 的范围要小. 本书第二版 (1988) 增加了 2045 个新的因子分解，反映了这期间在方法和技术上的重要进展. 最近出版的第三版列出 2332 个新的因子分解.

这个集体合作也戏称为“ Cunningham 计划”，起源于想把 Cunningham 和 Woodall 于 1925 年发表的表格加以扩大. 这项活

动可能会永无休止地继续下去！

Riesel(1985) 的书以很大篇幅讲述因子分解 (和素性判定). 其中包括费马数、Mersenne 数，形如 $2^n+1, 10^n+1, (10^n-1)/9$ 的数等的因子分解，并以易懂和统一的方式讲述因子分解技术方法. 由于这些内容受人欢迎，1994 年第二版中还增加了椭圆曲线因子分解的内容.

1989 年， Bressoud 出版一本关于因子分解和素性判定的大学生教科书，不仅包括基本内容，也讲到二次筛法和椭圆曲线方法.

在综述性文章中，下列工作值得注意： Guy(1975) 讨论现在称之为经典的一些方法；Williams(1984) 除了经典内容之外，自然加进那时的新内容，这是一本读起来令人愉快的书； Dixon(1984) 写了因子分解和素性判定； Pomerance(1984) 一个短课的讲义附有重要的文献.

至于更专业性的论文， Lenstra(1987) 论述用椭圆曲线做因子分解；他的兄弟 Lenstra(1990) 也是基础性的重要文章. 由 Lenstra, Manasse 和 Pollard(1993) 所写的是数域筛法文章.

作为一些例子，也为了满足大数分解爱好者的要求，我现在给出一些 Mersenne 数、费马数等的具体分解式. 这方面早期的参考书为 Dickson 的《数论史》第 I 卷第 22, 29, 377 页和 Archibald (1935).

1869 年 Landry 给出

$$M_{59}=2^{59}-1=179951\times 3203431780337$$

1903 年 Cole 得到

$$M_{67}=2^{67}-1=193707721\times 761838257287$$

1923 年 Poulet 得到

$$M_{73} = 2^{73} - 1 = 439 \times 2298041 \times 9361973132609$$

其中因子 439 是欧拉首先发现的. 1856 年 Clausen 得出

$$\begin{aligned} F_6 = 2^{2^6} + 1 &= (1071 \times 2^8 + 1) \times (262814145745 \times 2^8 + 1) \\ &= 274177 \times 67280421310721 \end{aligned}$$

以上分解式均是计算机时代之前算出的. 1947 年 Lehmer 得到分解式

$$M_{113} = 2^{113} - 1 = 3391 \times 23279 \times 65993 \times 1868569 \times 1066818132868207$$

其中最小素因子是 Reuschle 于 1856 年发现的. 1983 年, Naur, Pomerance 和 Wagstaff 独立地分解出

$$\begin{aligned} M_{193} = 2^{193} - 1 = &13821503 \times 61654440233248340616559 \\ &\times 14732265321145317331353282383 \end{aligned}$$

下一个分解式和 Mersenne 本身有直接的历史性联系 (见 2.7 节)

$$\begin{aligned} M_{257} = 2^{257} - 1 = &535006138814359 \\ &\times 1155685395246619182673033 \\ &\times 374550598501810936581776630096313181393 \end{aligned}$$

其中第一个因子和后两个因子分别由 Penk 和 Baillie 于 1979 和 1980 年发现. 注意 Lehmer 在 1927 年已证明 M_{257} 不是素数, 但是没有给出它的任何素因子.

现在又回到费马数. Morrison 和 Pollard 于 1970 年给出 (发表于 1971 年)

$$F_7 = 2^{2^7} + 1 = 59649589127497217 \times 5704689200685129054721$$

Brent 和 Pollard 于 1980 年给出 (发表于 1981 年)

$$F_8 = 2^{2^8} + 1 = 1238926361552897 \times 93461639715357977769163558199606896584051237541638188580280321$$

费马数 F_{11} 于 1988 年被完全分解，其中最小的两个素因子早已求出，接下来的两个素因子是由 Brent 用椭圆曲线方法得到的. Brent 认为剩下的 564 位数是素数，这由 F.Moràin 所证明.

F_9 于 1990 年由 A.K.Lenstra 和 M.S.Manasse 分解成功，采用了数域筛法. Brent 于 1995 年分解了费马数 F_{10}. 以上是费马数和 Mersenne 数的情况.

Dov Jarden,Brillhart,Montgomery 和 Silverman 于 1988 年列出 Fibonacci 数 U_n $(2 \nmid n \leqslant 999)$ 和 Lucas 数 V_n $(n \leqslant 500)$ 的所有已知的因子，并且分别对 $n \leqslant 387$ 和 $n \leqslant 397$ 的情形完全分解. 到了 2003 年 4 月， Montgomery 报告说，已经对 U_n 和 V_n 在 $n \leqslant 1000$ 之内完成了分解. 这项工作把 Jarden(见他书的第三版 1958 年) 等许多人的工作大大推进了一步.

下面是另一些值得介绍的分解式，它们为在大数分解方面的一些里程碑. 1984 年 Atkin 和 Rickert 分解了

$$\frac{10^{103}+1}{11} = 1237 \times 44092859 \times 102860539 \times 984385009 \times 612053256358933 \times 182725114866521155647161 \times 1471865453993855302660887614137521979$$

A.K.Lenstar 和 M.S.Manasse 于 1988 年 10 月 12 日 “愉快地宣布

把一个 100 位的数用一般型因子分解算法”分解了

$$\frac{11^{104}+1}{11^8+1} = 86759222313428390812218077095850708048977 \times 108488104853637470612961399842972948409834611525790577216753$$

算法是确定型的，只依赖于 N 的大小，不依赖于 N 的因子的任何特殊性质. 计算时间与平均时间一样.

数域筛法将 138 位的 $2^{457}+1$ 完全分解为 $3 \times P49 \times P89$, 其中 Pn 表示一个 n 位的素数. 这是 A.K.Lenstra 和 M.S.Manasse 于 1989 年 11 月完成的，为一种特殊数域筛法 (SNFS) 的一个成功的例子. 报纸以第一版报道了这一事件.

1992 年，A.K.Lenstra 和 D.Bernstein 用 SNFS 和两个超大级并行机，把 158 位的 Mersenne 数 M_{523} 分解成分别有 69 和 90 位的两个素因子之积.

1999 年 4 月，自称为“ Cabal ”的一个小组宣布一项超大级因子分解. 他们又使用 SNFS 把全 1 数 $(10^{211}-1)/9$ 分解成 $P93 \times P118$. 发现了当时最大的回文素数. 这个小组的成员为 S.Cavallar,B. Dodson, A. Lenstra, P. Leyland, W. Lioen, P. Montgomery, H. te Riele 和 P. Zimmermann.

下面一小节中我要介绍公钥密码体制，其中用到很难分解的大数.

为了对素性和分解有更深刻的理解，建议参看 Crandall 和 Pomerance(2001) 的一本新书. 此书中包括了最重要的方法和证明，两位作者均为该领域当前的权威.

对于素性检测、大数分解以及与大数有关的其他计算有兴趣的人，当然需要有最新一代的高速高性能计算机可供使用. 但是仍有一些原创性的工作是在个人电脑上发展出来的，所以我们还

可以在舒适的家中得到一些重要的成果. 如果外面在下雪 (这在加拿大是经常发生的), 你可以双脚保持暖和, 来检测你的素数.

2.11E 公钥密码体制

通信手段飞速进步, 传递信息的领域日益广泛深入, 从银行存款、朋友通信、购买股票, 一直到秘密外交和间谍活动, 均需要将信息编码的安全方法. 在过去, 信息编码后的密文只有发方和收方知道, 但是信息可以被外人截获, 密文被破译. 如果加密方式过于简单, 外人可以通过分析信息中每个字母出现的频率把密文破译, 这在战争中会造成非常严重的后果.

密码学的一个重大进步是发明了公钥密码体制. 这个体制的主要特点是简单, 使用公开密钥, 并且破译非常困难. 公钥思想是 Diffie 和 Hellman 于 1976 年提出, 而在 1978 年由 Rivest,Shamir 和 Adleman 给出有效的方案, 这种方案被称为 RSA 体制. 我现在介绍这种方案.

每个字母和符号 (包括空白) 都对应一个三位数. 在 "信息转换美国标准表编码 (ASCII) " 中, 这种对应为

–	A	B	C	D	E	F	G	H
032	065	066	067	068	069	070	071	072
I	J	K	L	M	N	O	P	Q
073	074	075	076	077	078	079	080	081
R	S	T	U	V	W	X	Y	Z
082	083	084	085	086	087	088	089	090

信息中每个字母和符号都改用代表它的 3 位数, 于是整个信息被编成一个数 M.

系统中的每个用户有公钥 (n_A, s_A), 其中 $n_A = p_A q_A$ 是两个

大素数的乘积， n_A 公开，但是它的两个素因子 p_A 和 q_A 保持秘密．进而，取正整数 s_A, 使得 s_A 和 p_A-1, q_A-1 均互素.

为把信息 M 传送给另一个用户 B,A 要把信息 M 加密，这是将 M 用收方 B 的公钥作用．用户 B 收到由 A 发送来的密文之后，用自己的私钥解密.

详言之，整个过程如下：若信息 $M \geqslant n_B$, 要把 M 分成一些小块，以下设 $M < n_B$. 若 $\gcd(M, n_B) \neq 1$, 可在信息末尾加上一个无意义的字母，使得对新的信息， $\gcd(M, n_B) = 1$.

A 把加密后的密文 $E_B(M) = M'$ 发给 B,$1 \leqslant M' < n_B$, 其中 $M' \equiv M^{s_B} \pmod{n_B}$. 为了将 M' 解密，用户 B 要计算出 t_B, $1 \leqslant t_B < (p_B-1)(q_B-1) = \varphi(n_B)$, 满足 $t_B s_B \equiv 1 \pmod{\varphi(n_B)}$, 这样的 t_B 一定可以求出来．然后

$$D_B(M') = M'^{t_B} \equiv M^{s_B t_B} \equiv M \pmod{n_B}$$

从而 B 读出明文信息 M. 事情就是如此简单！

当然，还会有一些技术性问题．这些问题已在专门性书籍和大量文章中加以讨论．我在这里只介绍其简化的思想，并用例子加以解释．为了更加方便，假设把信息中每两个数字作为一组，实际工作当然不是这样.

现在从你口袋里拿出你的计算器．下面为某人的一个密文

151474036925076974117964029299026654036925101743109701

095179152070068045055176008329001574149966031533117864

154599013907031533013986012353068045133750126510137349

117864113338128986117864110052047607001574010738003772

096642117864070838109145011098117864028600117864056547

117864083567041271109145056006

此密文发给一个收方，收方的公钥为 $(n, s) = (156287, 181)$. 你不知道 n 的秘密素因子. 你是否能够破译这个密文？答案印在本书的某个地方.

关于破译这个密码体制我还要再说几句. 每个用户 A 需要求出 $\varphi(n_A)$. 这件事等价于把 n_A 因子分解. 因为若知道了 n_A 的两个素因子 p_A 和 q_A, 则 $\varphi(n_A) = (p_A - 1)(q_A - 1)$. 反过来，令 $p = p_A$, $q = q_A$, $n = n_A$. 由 $\varphi(n) = (p-1)(q-1) = n+1-(p+q)$ 和 $(p+q)^2 - 4n = (p-q)^2$(设 $p > q$) 可得

$$p + q = n + 1 - \varphi(n)$$

$$p - q = \sqrt{[n + 1 - \varphi(n)]^2 - 4n}$$

即 p 和 q 可由 n 和 $\varphi(n)$ 求出.

关于 RSA 公钥体制还有很多问题. 比如说:

(1) 如何传输“签名”的信息，使收方能确认这个信息确实来自发方;

(2) 如何选择密钥 n_A 的素因子，使得破译这个公钥体制采用现有的方法是不可行的.

对于问题 (2), 信息安全最重要的事情中，首先是密钥 n_A 不能被分解. 那么密钥 n_A 需要多少位才可在有效时间之内不能被分解？

为了检测此事，数学家建议各种密钥来比赛它们的分解. 其中有一个叫作 RSA-155 的数 (表示它有 155 位)

RAS-155 =10941738641570527421809707322040357612003732945449205990913842131476349984288934784717997257891267332497625752899781833797076537244027146743531593354333897

这个数是精心构作出来的，想成为 RSA 方法中可能的密钥. 1999 年 8 月，由 H.te Riele 领导六个国家的科学家组成的小组把此数分解，用一般的数域筛法把它分解成以下两个 78 位的素数之乘积

1026395928297411057720541965739916759007165678080380668033419335217907113077779

1066034883801684548209272203600128786792079585759892915222706082371930628086643

这个破译比 RSA 方法刚开始采用时所预计的时间要早很多. 这表明 512 比特 (即十进制 155 位) 的公钥已不再安全. 目前建议用 768 比特 (十进制 230 位) 的公钥作为达到安全可靠的最低标准，并且其素因子 p 和 q 要随机选取并且大小相近.

目前作为 RSA 因子分解挑战的数从 RSA-576(576 比特，十进制 174 位) 到 RSA-2048(2048 比特，十进制 617 位). 而奖金从一万美元到二十万美元.

关于以上这些问题的原始文章为 Rivest,Shamir,Adleman(1978) 和 Rivest(1978) 所写. 还有综述文章为 Couvreur 和 Quisquater (1982) 作者的，以及以下一些所写书籍： Riesel (1985), Koblitz (1987), Bressoud (1989), Coutinho (1999) 和 Wagstaff(2003). 还有 Lemos 用葡萄牙文写的讲义 (1989), 很像是用加密语言来介绍密码学.

第三章　是否有定义出素数的函数？

为了决定出素数，一个自然的问题是：是否有实际可计算的函数 f，使得对所有自然数 $n \geqslant 1$，函数值 $f(n)$ 均为素数，甚至由此得到全部素数？

例如，函数应当满足下列条件中的某一个：

(a) 对每个 $n \geqslant 1$，$f(n) = p_n$(第 n 个素数)；

(b) $f(n)$ 均是素数，并且当 $n \neq m$ 时，$f(n) \neq f(m)$；

(c) 素数集合等于函数在正整数处取值组成的集合.

显然，条件 (a) 比 (b) 和 (c) 都强.

除了对条件 (c) 有一些结果在理论上是重要的，目前得到的其余结果相当令人失望.

3.1　满足条件 (a) 的函数

Hardy 和 Wright 在他们著名的书中问道：

(1) 对于第 n 个素数是否有公式？

(2) 是否存在用一个素数前面的所有素数来表达这个素数的公式？

问题 (1) 的意思是：求一个明确的表达式 f，使得 $f(n)$ 等于第 n 个素数 p_n，并且函数 f 是可计算的，而且 f 尽可能表示成熟知的函数形式. 与此问题密切相关的另一个问题是：对于计算素数个数的函数 $\pi(x)$ 给出一个好的表达式. 这里对每个实数 $x > 0$，$\pi(x)$ 表示不超过 x 的素数的个数.

$\pi(x)$ 是素数理论中一个重要函数，并且记号也是传统的．我在第四章要进一步讲述这个函数．即使数 $\pi = 3.14\cdots$ 和函数 $\pi(x)$ 在以后会出现在同一个公式之中，其意义也不会混淆．

首先我要介绍 Willans 在 1964 年给出的关于 $\pi(m)$ 的一个公式，它是基于我在第二章证明的 Wilson 定理．

对每个整数 $j \geqslant 1$, 令

$$F(j) = \left[\cos^2 \pi \frac{(j-1)!+1}{j}\right]$$

这里对实数 x,$[x]$ 表示满足 $n \leqslant x < n+1$ 的唯一的整数 n.

于是对每个整数 $j > 1$, 当 j 为素数时 $F(j) = 1$, 否则 $F(j) = 0$, 并且 $F(1) = 1$. 因此

$$\pi(m) = -1 + \sum_{j=1}^{m} F(j)$$

Willans 还把 $\pi(m)$ 表示成

$$\pi(m) = \sum_{j=2}^{m} H(j) \qquad (m = 2, 3, \cdots)$$

其中

$$H(j) = \frac{\sin^2 \pi \frac{((j-1)!)^2}{j}}{\sin^2 \frac{\pi}{j}}$$

Mináč 给出另一个表达式 (未发表), 其中正弦和余弦均不出现在公式中

$$\pi(m) = \sum_{j=2}^{m} \left[\frac{(j-1)!+1}{j} - \left[\frac{(j-1)!}{j}\right]\right]$$

证明　这个公式的证明很简单，由于它没有发表，我这里给出它的证明．

首先注意：若 $n \neq 4$ 不是素数，则 n 除尽 $(n-1)!$. 这是因为，n 或者写成 $n = ab$, 其中 $2 \leqslant a, b \leqslant n-1$ 并且 $a \neq b$, 或者 $n = p^2 \neq 4$. 对于前者，n 除尽 $(n-1)!$; 对于后者，$2 < p \leqslant n-1 = p^2-1$, 从而 $2p \leqslant p^2-1$. 于是 n 除尽 $2p^2 = p \times 2p$, 从而 n 除尽 $(n-1)!$.

根据 Wilson 定理，对每个素数 j,$(j-1)!+1 = kj$, 其中 k 为整数，于是

$$\left[\frac{(j-1)!+1}{j} - \left[\frac{(j-1)!}{j}\right]\right] = \left[k - \left[k - \frac{1}{j}\right]\right] = 1$$

若 j 不是素数并且 $j \geqslant 6$, 则 $(j-1)! = kj$, 其中 k 为整数. 由上面注记可知

$$\left[\frac{(j-1)!+1}{j} - \left[\frac{(j-1)!}{j}\right]\right] = \left[k + \frac{1}{j} - k\right] = 0$$

最后对 $j = 4$, 则

$$\left[\frac{3!+1}{4} - \left[\frac{3!}{4}\right]\right] = 0$$

这就证明了 $\pi(m)$ 的这个公式. □

利用前面的记号，Willans 对于第 n 个素数给出以下公式：

$$p_n = 1 + \sum_{m=1}^{2^n} \left[\left[\frac{n}{\sum_{j=1}^{m} F(j)}\right]^{\frac{1}{n}}\right]$$

或者用函数 $\pi(x)$ 来表达

$$p_n = 1 + \sum_{m=1}^{2^n} \left[\left[\frac{n}{1+\pi(m)}\right]^{\frac{1}{n}}\right]$$

设 p 是素数 q 的前一个素数，Willans 给出用 p 表达 q 的公式

$$q = 1 + p + F'(p+1) + F'(p+1)F'(p+2) + \cdots + \prod_{j=1}^{p} F'(p+j)$$

其中 $F'(j)=1-F(j)$, 而 $F(j)$ 的定义如前所示.

Ernvall 对于大于 $m(\geqslant 2)$ 的最小素数给出另一个公式，他的这个公式发表于 1975 年，当时他还是个学生. 令

$$\begin{aligned} d &= \gcd\left((m!)^{m!}-1,\ \ (2m)!\right) \\ t &= \frac{d^d}{\gcd(d^d, d!)} \end{aligned}$$

而 a 是唯一的整数，使得 d^a 除尽 t, 但是 d^{a+1} 除不尽 t, 则大于 m 的最小素数为

$$p=\frac{d}{\gcd(t/d^a, d)}$$

取 $m=p_{n-1}$, 它给出 p_n 的一个公式.

尽管这些公式没有太大的实用价值，我还是相信它们对于逻辑学家有些用途：逻辑学家试图清楚地理解算术的不同内容是由不同的公理系统演绎出来的，还是均由皮亚诺算术公理得出.

1971 年， Gandhi 给出 p_n 的一个公式. 为了解释这个公式，我们需要 Möbius 函数，它定义为

$$\begin{cases} \mu(1)=1 \\ \mu(n)=(-1)^r, \text{若 } n \text{ 是 } r \text{ 个不同素数的乘积} \\ \mu(n)=0, \text{若某个素数的平方除尽 } n \end{cases}$$

令 $P_{n-1}=p_1p_2\cdots p_{n-1}$,Gandhi 证明了

$$p_n=\left[1-\frac{1}{\lg 2}\lg\left(-\frac{1}{2}+\sum_{d|P_{n-1}}\frac{\mu(d)}{2^d-1}\right)\right]$$

或者等价地说， p_n 是满足

$$1<2^{p_n}\left(-\frac{1}{2}+\sum_{d|P_{n-1}}\frac{\mu(d)}{2^d-1}\right)<2$$

的唯一整数.

下面的证明是 Vanden Eynden 于 1972 年给出的.

证明 为简化记号，令 $Q = P_{n-1}$，$p_n = p$, 而

$$S = \sum_{d|Q} \frac{\mu(d)}{2^d - 1}$$

于是

$$(2^Q - 1)S = \sum_{d|Q} \mu(d) \frac{2^Q - 1}{2^d - 1} = \sum_{d|Q} \mu(d)(1 + 2^d + 2^{2d} + \cdots + 2^{Q-d})$$

如果 $0 \leqslant t < Q$, 则 $\mu(d)2^t$ 这项出现在求和之中当且仅当 d 除尽 $\gcd(t, Q)$. 从而在后一个和号中 2^t 的系数为 $\sum\limits_{d|\gcd(t,Q)} \mu(d)$. 当 $t = 0$ 时，它为 $\sum\limits_{d|Q} \mu(d)$.

但是对每个整数 $m \geqslant 1$, 熟知 (也容易证明)

$$\sum_{d|m} \mu(d) = \begin{cases} 1, & m = 1 \\ 0, & m > 1 \end{cases}$$

以 $\sum\limits_{0<t<Q}{}'$ 表示对满足条件 $0 < t < Q$ 和 $\gcd(t, Q) = 1$ 的 t 求和，则 $(2^Q - 1)S = \sum\limits_{0<t<Q}{}' 2^t$. 求和式中最大 t 值为 $t = Q - 1$. 因此

$$2(2^Q - 1)\left(-\frac{1}{2} + S\right) = -(2^Q - 1) + \sum_{0<t<Q}{}' 2^{t+1} = 1 + \sum_{0<t<Q-1}{}' 2^{t+1}$$

如果 $2 \leqslant j < p_n = p$, 存在某个素数 q, 使得 $q < p_n = p$(从而 $q \mid Q$) 并且 $q \mid Q - j$. 于是上面和式中每个 t 都满足 $0 < t \leqslant Q - p$. 所以容易给出下面一些不等式:

$$\frac{2^{Q-p+1}}{2 \times 2^Q} < -\frac{1}{2} + S = \frac{1 + \sum\limits_{0<t\leqslant Q-p}{}' 2^{t+1}}{2(2^Q - 1)} < \frac{2^{Q-p+2}}{2 \times 2^Q}$$

乘以 2^p 之后，给出

$$1 < 2^p\left(-\frac{1}{2}+S\right) < 2 \qquad \square$$

Golomb 于 1974 年给出另一个证明，我认为这个证明富有启发性．他的证明是在 1 的二进制展开上作 Eratosthenes 筛法 (见第二章 2.1 节).

将每个正整数 n 赋予一个概率 (或叫作权)$W(n)=2^{-n}$. 显然 $\sum\limits_{n=1}^{\infty} W(n)=1$. 对于这个分布，是某个固定整数 $d \geqslant 1$ 的倍数的随机整数有概率

$$M(d)=\sum_{n=1}^{\infty} W(nd)=\sum_{n=1}^{\infty} 2^{-nd}=\frac{1}{2^d-1}$$

而与一个固定整数 $m \geqslant 1$ 互素的随机整数，其概率容易计算为

$$\begin{aligned} R(m) &= 1-\sum_{p|m} M(p)+\sum_{pp'|m} M(pp')-\sum_{pp'p''|m} M(pp'p'')+\cdots \\ &= \sum_{d|m}\mu(d)M(d)=\sum_{d|m}\frac{\mu(d)}{2^d-1} \end{aligned}$$

令 $Q=p_1p_2\cdots p_{n-1}$, 则

$$R(Q)=\sum_{d|Q}\frac{\mu(d)}{2^d-1}$$

但是另一方面，对于这个分布，可直接给出

$$R(Q)=\sum_{\gcd(m,Q)=1} W(m)=\frac{1}{2}+\frac{1}{2^{p_n}}+\frac{1}{2^{p_{n+1}}}+\alpha$$

α 是 2 的某些更高方幂的倒数和．因此

$$R(Q)-\frac{1}{2}=\sum_{d|Q}\frac{\mu(d)}{2^d-1}-\frac{1}{2}=\frac{1}{2^{p_n}}+\frac{1}{2^{p_{n+1}}}+\alpha$$

所以

$$2^{p_n}\left(\sum_{d|Q}\frac{\mu(d)}{2^d-1}-\frac{1}{2}\right)=1+\theta_n$$

其中 $0<\theta_n<1$. 从而 p_n 是满足

$$1<2^m\left(\sum_{d|Q}\frac{\mu(d)}{2^d-1}-\frac{1}{2}\right)<2$$

的唯一整数 m. 这就给出 Gandhi 公式的又一个证明. 由 $p_{n+1}\geqslant p_n+2$ 可知 $0<\theta_n<\frac{1}{2}$.

用二进制记号, 这些会变得更加透彻. 由于 $W(n)=0.000\cdots1$ (在第 n 位为数字 1), 所以 $\sum\limits_{n=1}^{\infty}W(n)=0.111\cdots=1$.

对于偶整数情形

$$\sum_{n=1}^{\infty}W(2n)=0.010101\cdots=\frac{1}{2^2-1}=\frac{1}{3}$$

相减则给出 $P_1=p_1=2$ 的公式

$$R(P_1)=\sum_{2|n}W(n)=0.101010\cdots=1-\frac{1}{3}$$

再减去 3 的倍数, 然后把减了两次的 6 的倍数加回来一次, 得到

$$Q(3)=0.001001001\cdots=\frac{1}{2^3-1}=\frac{1}{7}$$
$$Q(6)=0.000001000001\cdots=\frac{1}{2^6-1}=\frac{1}{63}$$

从而对于 $P_2=p_1p_2=6$, 有

$$\begin{aligned}R(P_2)=R(P_1)-Q(3)+Q(6)&=0.1000101000101000\cdots\\&=1-\frac{1}{3}-\frac{1}{7}+\frac{1}{63}\end{aligned}$$

继续下去，便得出

$$R(P_{n-1}) = 0.100\cdots0100\cdots0100\cdots = \frac{1}{2} + \frac{1}{2^{p_n}} + \frac{1}{2^{p_{n+1}}} + \alpha$$

$$R(P_{n-1}) - \frac{1}{2} = 0.000\cdots010\cdots$$

其中第一个 1 出现在位置 p_n 处.

3.2 满足条件 (b) 的函数

对于每个 $n \geqslant 1$, $f(n) = \left[\theta^{3^n}\right]$ 为素数,这里 θ 大致为 $1.3064\cdots$ (见 Mills 1947 年文章). 类似地，对每个 $n \geqslant 1$

$$g(n) = \left[2^{2^{2^{\cdot^{\cdot^{\cdot 2^w}}}}}\right] \qquad (\text{共有}n\text{个指数})$$

为素数，其中 w 大致为 $1.9287800\cdots$(见 Wright 1951 年文章).

θ 和 w 只知道近似值并且 $f(n)$ 和 $g(n)$ 增长得很快，这使得上述两个公式更显得奇妙. 如 $g(1) = 3, g(2) = 13, g(3) = 16381$, 而 $g(4)$ 比 5000 位数还大. 在文献中还有与之类似的其他公式，但这些公式好处不大，见 Dudley 1969 年文章.

在这里人们会问：为什么不用整系数的多项式来代替用指数函数和整数部分所造出的这类神秘的函数？ 3.3 节就讨论此事.

3.3 产生素数的多项式

对于上节末尾提出的问题，答案如下:

如果 $f(x)$ 是整系数单变量多项式并且不为常数，则存在无限多个整数 n, 使得 $|f(n)|$ 不是素数.

证明 不妨设存在整数 $n_0 \geqslant 0$, 使得 $|f(n_0)| = p$ 为素数. 由于多项式不为常数, 可知 $\lim\limits_{x\to\infty} |f(x)| = \infty$, 从而存在 $n_1 > n_0$, 使得当 $n \geqslant n_1$ 时, $|f(n)| > p$. 对任何满足 $n_0 + ph \geqslant n_1$ 的 $h, f(n_0+ph) = f(n_0) + (p\text{的倍数}) = p\text{的倍数}$. 但是 $|f(n_0+ph)| > p$, 所以 $|f(n_0+ph)|$ 不是素数. □

上面的命题是哥德巴赫于 1743 年 9 月 28 日给欧拉的信中指出来的.

于是, 没有整系数单变量多项式能满足我们的目的. 那么, 能否用多变量多项式呢? 答案仍是否定的, 并且有如下更强的否定结果:

若 $f(X_1, X_2, \cdots, X_m)$ 为 m 变量复系数多项式, 使得对任何整数 $n_1, n_2, \cdots, n_m, |f(n_1, n_2, \cdots, n_m)|$ 均为素数, 则 f 必为常数.

对于每个非常值的整系数单变量多项式 $f(X)$, 它在无限多自然数处的取值均不是素数. 但既使如此, 欧拉于 1772 年还是发现一个这样的多项式 $f(X)$, 它在许多连续整数处取值均为素数.

以下是欧拉的著名例子: $f(X) = X^2 + X + 41$, 是欧拉给 Bernoulli 的信中说到的. 对于 $k = 0, 1, 2, 3, \cdots, 39$, 这个多项式的取值均为素数, 即分别为 41, 43, 47, 53, 61, 71, 83, 97, 113, 131, 151, 173, 197, 223, 251, 281, 313, 347, 383, 421, 461, 503, 547, 593, 641, 691, 743, 797, 853, 911, 971, 1033, 1097, 1163, 1231, 1301, 1373, 1447, 1523, 1601. 而对 $k = 40$, 此多项式的取值为 $1681 = 41^2$.

这个例子推动了人们对以下问题作新的研究:

(1) 用较为系统的方法寻求一次、二次或更高次的多项式 $f(X)$, 使得对尽可能大的 $k > 0$, $|f(0)|, |f(1)|, \cdots, |f(k)|$ 均为素数.

(2) 如何判断一个多项式, 使得它在 (不必连续的) 许多整数处取值的绝对值均为素数.

我们首先考虑一次多项式．而对二次多项式情形，这个问题与二次域的算术性质有密切联系．所以为了方便，我要用一小节专门讨论这件事．对于次数大于 2 的多项式，这方面的结果知道得很少，见第六章 6.2 节．

3.3A 一次多项式的素数取值

设 $f(X)=dX+q$, 其中 $d>1, q>1$ 并且 $\gcd(d,q)=1$. 如果 $f(0)$ 是素数，则 q 为素数而 $f(q)$ 不是素数．所以对于一次多项式，至多有连续 q 个值为素数．这就产生了一个问题：是否对每个素数 q 均存在整数 $d \geqslant 1$, 使得 $q, d+q, 2d+q, \cdots, (q-1)d+q$ 均为素数？例如

$$q=3, d=2 \text{给出素数} 3,5,7$$

$$q=5, d=6 \text{给出素数} 5,11,17,23,29$$

$$q=7, d=150 \text{给出素数} 7,157,307,457,607,757,907$$

这个问题相当困难．我相信在不远的将来没人能证明它．注意： Lagrange 曾经证明了：如果这样的 d 存在，则 d 被 $\prod_{p<q} p$ 除尽．

1986 年， G.Löh 发现对 $q=11$, 最小的 d 值为 1536160080, 而对 $q=13$, 最小的 d 值为 9918821194590 .

记录

对于 $q=17$, 最小的 $d=341976204789992332560$, 是 P. Carmody 于 2001 年 11 月得到的．这是又一个惊人的计算结果！

我在第四章 4.5 节中将会再来考察关于算术级数中的素数和其他问题．

3.3B 关于二次域

为了理解关于二次多项式的上述问题，现在需要介绍一下所需要的二次域知识. 这些材料可以在许多数论书中找到，所以在这里不必做专门的评价. 高斯在他名著《算术探究》(1801) 中开创的二元二次型经典理论也有不少现代出版的书中加以叙述，例如， Flath(1989) 的书和我的书 *My Numbers, My Friends* (2000) 中很长的一章. 这里我只提及今后所需的内容.

设 $d \neq 0,1$ 为无平方因子整数 (可正可负). 它结合一个 (基本) 判别式

$$\Delta = \begin{cases} d, & d \equiv 1 \pmod 4 \\ 4d, & d \equiv 2,3 \pmod 4 \end{cases}$$

然后又结合一个二次域 $\mathbb{Q}(\sqrt{d}\,) = \mathbb{Q}(\sqrt{\Delta}) = \left\{r + s\sqrt{d} \mid r, s \in \mathbb{Q}\right\}$. 当 $d > 0$ 时， $r+s\sqrt{d}$ 均为实数， $\mathbb{Q}(\sqrt{d}\,)$ 叫 **实二次域**. 而当 $d < 0$ 时， $\mathbb{Q}(\sqrt{d}\,)$ 叫 **虚二次域**.

$\mathbb{Q}(\sqrt{d}\,)$ 中的每个元素 α 是 $\mathbb{Q}[x]$ 中某个二次多项式 (如果 α 不属于 $\mathbb{Q}$) 或一次多项式 (若 α 属于 $\mathbb{Q}$) 的根，并且可取此多项式 $f(x)$ 最高次项系数为 1. 如果 $f(x)$ 的系数均属于 $\mathbb{Z}$, 则 α 叫作 $\mathbb{Q}(\sqrt{d}\,)$ 中的 **代数整数**. 全体代数整数组成的集合 A 是 $\mathbb{Q}(\sqrt{d}\,)$ 的一个子环. 容易刻画 A 中的元素

$$\text{若}d \equiv 1 \pmod 4,\quad \text{则}A = \left\{\frac{1}{2}(m + n\sqrt{d}\,) \mid m, n \in \mathbb{Z},\ 2|m-n\right\}$$

$$\text{若}d \equiv 2,3 \pmod 4,\quad \text{则}A = \left\{m + n\sqrt{d} \mid m, n \in \mathbb{Z}\right\}$$

对于每个 $n \geqslant 1$ 和 $\alpha_1, \alpha_2, \cdots, \alpha_n \in \mathbb{Q}(\sqrt{d}\,)$, 集合 $\left\{\sum\limits_{i=1}^{n} \gamma_i\alpha_i \mid \gamma_1, \cdots, \gamma_n \in A\right\}$ 叫作由 $\alpha_1, \alpha_2, \cdots, \alpha_n$ 生成的 **分式理想**. 如果 I 是一个分式理想，则 $I + I \subseteq I$ 并且 $AI \subseteq I$. 特别地，对每个

$\alpha \in \mathbb{Q}(\sqrt{d}\,)$, $A\alpha$ 是分式理想，这叫作 **主分式理想**. 若 I 和 J 是分式理想，定义它们的乘积为

$$IJ = \left\{ \sum_{i=1}^{n} \alpha_i \beta_i \mid \alpha_i \in I, \beta_i \in J, n \geqslant 0 \right\}$$

这也是分式理想. 所以非零分式理想对于这个乘法形成一个交换群，而所有非零的主分式理想形成它的一个子群.

高斯 (用不同的但与之等价的语言) 证明了：非零分式理想群对于非零主分式理想子群的商群是有限交换群. 表示成 Cl_d(或 Cl_Δ), 叫作 $\mathbb{Q}(\sqrt{d}\,)$(或 Δ) 的 **类群**. 这个群的元素个数表示成 h_d(或 h_Δ), 叫作 $\mathbb{Q}(\sqrt{d}\,)$ (或 Δ) 的 **类数**. 所以，类数等于 1 相当于说每个分式理想都是主分式理想.

如果 $\alpha, \beta \in \mathbb{Q}(\sqrt{d}\,)$, 定义 α **整除** β 是指存在 $\gamma \in A$ 使得 $\alpha\gamma = \beta$.A 中整除 1 的元素叫作 A 中的 **单位**.A 中非零元素 π 叫作是 **素代数整数**, 是指 π 不是单位，并且若 $\pi = \alpha\beta$,α 和 β 均属于 A, 则 α 或 β 必有一个为单位.

可以证明： $h_d = 1$ 当且仅当 $\mathbb{Q}(\sqrt{d}\,)$ 中存在唯一因子分解定理，即每个非零代数整数均可表示成素代数整数的乘积，并且不考虑因子的次序和相差单位因子，这种表示法是唯一的.

类群 Cl_d 的 **指数** e_d 是群 Cl_d 中每个元素 (叫作理想类) 阶的最大值. 这时，每个理想类的阶都是 e_d 的因子. 当然 $e_d = 1$ 当且仅当 $h_d = 1$, 并且 e_d 为 2 的方幂当且仅当 h_d 为 2 的方幂.

高斯所发展的二元二次型种 (genera) 理论可给出更精细的结果. 令

$$h_d^* = \begin{cases} h_d, & d < 0 \\ 2h_d, & d > 0 \end{cases}$$

又令 $N+1$ 为 Δ 的不同素数因子的个数. 高斯证明了 2^N 整除 h_d^*. 并且若 $d < 0, e_d = 1$ 或 2, 则 $h_d = 2^N$.

由此可知，对于 $d<0$ 的情形，当 $h_d=1$ 时， $N=0$, 从而 $d=-1,-2$ 或 $-p$, 其中 p 为素数并且 $d\equiv 3(\mathrm{mod}\ 4)$. 当 $h_d=2$ 时， $N=1$ 而 d 有以下三种可能性：

(i) $d=-2p$, 其中 p 为奇素数；

(ii) $d=-p$, 其中 p 为素数， $p\equiv 1(\mathrm{mod}\ 4)$;

(iii) $d=-pq$, 其中 p 和 q 为素数， $p<q$, $pq\equiv 3(\mathrm{mod}\ 4)$.

具有给定判别式的所有二元二次型 ⑤(对于某种运算) 也形成一个有限交换群 ⑥, 这个群与群 Cl_Δ 有确定的联系，这里不再解释其联系的方式. 二元二次型分成一些种，每个种包含一定数量的类. 种的理论可以推出下列两个命题是等价的：

对于 $d<0$,

(1) 判别式为 d 的二元二次型的类群有指数 1 或 2;

(2) 判别式为 d 的二元二次型类群的每个种均只包含一个类.

后一个性质可以用欧拉的术语“宜数” (拉丁文 numeri idonei, 英文 convenient number) 来解释. 这种数的定义如下.

设 $n\geqslant 1$, 以 $E(n)$ 表示具有下列性质的所有奇数 $q\geqslant 1$ 组成的集合：存在至多一对非负整数 (x,y), 使得 $q=x^2+ny^2$ 并且 $\gcd(x,ny)=1$. 数 n 叫作 **宜数**, 是指集合 $E(n)$ 中没有合成数 (即没有大于 1 的非素数).

例如，费马对形如 x^2+y^2 的整数加以研究，结果表明 1 是宜数. 高斯证明了：若 $d<0$, 则 $e_d=1$ 或者 2, 当且仅当 $-d$ 为宜数. 欧拉给出下列 65 个宜数：

$$1,2,3,4,5,6,7,8,9,10,12,13,15,16,18,21,22,24,$$
$$25,28,30,33,37,40,42,45,48,57,58,60,70,72,78,85,$$
$$88,93,102,105,112,120,130,133,165,168,177,190,$$

---

⑤ 应为二元二次型的类 —— 译者注.

⑥ 叫作二元二次型的类群 —— 译者注.

$$210, 232, 240, 253, 273, 280, 312, 330, 345, 357, 385, 408,$$
$$462, 520, 760, 840, 1320, 1365, 1848$$

完全决定所有宜数的问题至今没有解决. 已经证明了除上述宜数之外, 至多还有一个宜数. 事实上, 人们相信不再有那个例外的宜数, 即上面的 65 个宜数是全部清单.

现在讨论下一个问题: 对每个固定 $h \geqslant 1$, 决定 $h_d = h$ 的全部虚二次域 $\mathbb{Q}(\sqrt{d}\,)$

(1) 高斯证明了当 $d = -1, -2, -3, -7, -11, -19, -43, -67$ 和 -163 时, $h_d = 1$. 他 (在上述名著第 303 节中) 猜想 $h_d = 1$ 的虚二次域只有上述九个. (准确地说, 高斯并不是研究虚二次域, 而是讨论判别式小于 0 并且只有一类的二元二次型.)

1934 年, Heibronn 和 Linfoot 在一篇经典文章中证明了: 类数为 1 的虚二次域至多还有一个. 而 Lehmer(1933) 就已经证明了: 若类数 1 的新虚二次域 $\mathbb{Q}(\sqrt{d}\,)$ 存在, 必然 $|d| > 5 \times 10^9$. Heegner 在 1952 年证明了不存在这样的 d, 但是他的证明中有几步不够清楚, 甚至可能是错的.

Baker 在 1966 年证明了同样的结论, 他的证明利用了三个对数的线性型的有效下界估计. 还可见他 1971 年的文章. 几乎在同时, Stark(1967) 对于椭圆模函数采用 Heegner 的类似想法证明了新 d 值的不存在性, 于是便完全决定了类数 $h_d = 1$ 的虚二次域共有九个.

在这之后, Deuring 于 1968 年完善了 Heegner 的证明, 而 Stark (1969) 指出, Gelfond 和 Linnik 利用 1949 年所知道的关于两个对数的线性型结果, 就可以得到同样的结论. 这个证明的技术细节超出了本书的范围.

(2) Baker(1971) 用他关于对数线性型下界的方法, 证明了类数 $h_d = 2$ 的虚二次域也可以有效地决定, 但是他没有给出判别式

的明确上界. 在同一个杂志的同一卷中， Stark 计算了当 $h_d = 2$ 时， $|d| < 10^{1100}$.Montgomery 和 Weinberger 于 1974 年证明了在 $10^{12} \leqslant |d| \leqslant 10^{1200}$ 时， $h_d \neq 2$. 更早些时候， Lehmer 验证了 $10^6 \leqslant |d| \leqslant 10^{12}$ 时 $h_d \neq 2$.

将这些努力合在一起，便知 $d < 0$ 和 $h_d = 2$ 时，一共有 18 个判别式 $d = -5, -6, -10, -13, -15, -22, -35, -37, -51, -58, -91, -115, -123, -187, -235, -267, -403, -427$.

对于 $e_d = 2$ 的全部 $d < 0$ 至今仍未完全决定出来， Weinberger 于 1973 年对此给出 $|d|$ 的一个有效的上界.

(3) 关于任意的 h_d 值，高斯猜想，对每个 $n \geqslant 1$，均只有有限多虚二次域 $\mathbb{Q}(\sqrt{d}\ )$ 使得 $h_d = n$. 这个猜想由 Gross 和 Zagier(1983,1986) 所证明，其中利用 Goldfeld(1977) 一个突破性的结果，是下面更精确结果的一个推论.

对每个 $\varepsilon > 0$，存在可有效决定的 $C = C(\varepsilon) > 0$，使得 $d < 0$ 时， $h_d > C(\lg|d|)^{1-\varepsilon}$.

实二次域类数的研究要困难得多. 这里只提及高斯的另一个猜想：类数 $h_d = 1$ 的实二次域有无限多个. 这个猜想若被证明，将是一个重大的成果.

3.3C 产生素数的二次多项式

为方便起见，我们把一个二次多项式 $f(X) = aX^2 + bX + c$ $(a, c \geqslant 1)$ 叫作是 **产生素数的多项式**，是指存在 $l > 2$，使得 $f(0), f(1), \cdots, f(l-1)$ 均为素数. 本节一开始已指出这样的 l 是有上界的. l 的最大值叫作 $f(x)$ 的 **素数生成长度**.

我们即将看到，产生素数的多项式和二次域的类数有奇妙的关系. 这一小节就讨论这种关系. 但是还有一种完全不同类型的关系和关于素数的 k 元组猜想相联系，见第四章 4.4 节.

考虑多项式 $f_q(X)=X^2+X+q$, 其中 q 为素数. 注意 $f(q-1)=q^2$.Rabinowitsch 于 1912 年证明了下面两个命题是等价的:

(1) $f_q(X)$ 的素数生成长度为 $q-1$;

(2) 虚二次域 $\mathbb{Q}(\sqrt{1-4q}\,)$ 的类数为 1.

在同一年, Frobenius 证明了由 (2) 可推出 (1). 我发现 Lehmer 1936 年证明了由 (1) 可推出 (2). 而后来 Szekeres(1974) 和 Ayoub, Chowla (1981) 又证明了由 (2) 可推出 (1). 这个结果的详细讨论可见 Cohn 的书 (1962) 或者我的文章 (1988). 在那里, 从基本原则出发, 所有的计算和证明细节都交待清楚.

由于类数 1 的虚二次域已经完全决定, 从而可给出全部可能的 q 值. 事实上, 上面列出的九个 d 值中, 除了 -1 和 -2 之外均模 4 同余 1. 在其中除了 -3 之外, $(1-d)/4$ 均为素数 q. 于是给出 $q=2,3,5,11,17,41$. 所以当且仅当 q 为这六个素数的时候, $f_q(X)$ 是素数生成长度为 $q-1$ 的多项式. 这就给出下面的一个最佳记录.

记录

对于形如 X^2+X+q 的多项式, 欧拉已给出最好的结果: $q=41$ 是最大的素数, 使得 X^2+X+q 在 $X=0,1,\cdots,q-2$ 处的取值均为素数.

存在着许多二次多项式具有更大的素数生成长度. 勒让德证明当 $q=3,5,11,29$ 时, 多项式 $2X^2+q$ 的素数生成长度为 q(这是最大可能).A.Lévy 在 1914 年发现 $3X^2+3X+23$ 的素数生成长度为 22, 而 van del Pol 和 Speziali 于 1951 年提到 $6X^2+6X+31$ 的素数生成长度为 29. 这些例子引发出一个结果, 现在我解释这个结果.

根据类数 2 的三种虚二次域类型，定义

$f_{\mathrm{I}}(X)=2X^2+p$,　p为奇素数

$f_{\mathrm{II}}(X)=2X^2+2X+\dfrac{p+1}{2}$,　p为奇素数,$p\equiv 1(\mathrm{mod}\ 4)$

$f_{\mathrm{III}}(X)=pX^2+pX+\dfrac{p+q}{2}$,　p 和 q 为奇素数，$p<q,pq\equiv 3(\mathrm{mod}\ 4)$

注意 $f_{\mathrm{I}}(p),f_{\mathrm{II}}((p-1)/2)$ 和 $f_{\mathrm{III}}((p+q)/4-1)$ 均为合成数. 下列结果是 Louboutin(1991) 给出的，还见 Frobenius(1912) 和 Hardy (1974).

(I) $h_{-2p}=2$ 当且仅当 $f_{\mathrm{I}}(X)$ 的素数生成长度为 p；

(II) $h_{-p}=2$ 当且仅当 $f_{\mathrm{II}}(X)$ 的素数生成长度为 $(p-1)/2$；

(III) $h_{-pq}=2$ 当且仅当 $f_{\mathrm{III}}(X)$ 的素数生成长度为 $(p+q)/4-1$.

与 $h_d=2$ 的虚二次域清单加以比较，对三种情形得到：

(I) $p=3,5,11,29$；

(II) $p=5,13,37$；

(III) $(p,q)=(3,5),(3,17),(3,41),(3,89),(5,7),(5,23),(5,47),$
$(7,13)(7,61),(11,17),(13,31).$

Louboutin 在 1991 年同一文章中对于类数为 4 的虚二次域给出如下的刻画. 设 p 和 q 为素数，$2<q<p$. 则

(1) $h_{-2pq}=4$ 当且仅当对所有 $k=0,1,\cdots,p-1,2qk^2+p$ 均为素数.

(2) 设 $pq=1(\mathrm{mod}\ 4)$. 则 $h_{-pq}=4$ 当且仅当 $(pq+1)/2$ 为素数，并且对于 $k=0,1,\cdots,(p+q)/2-2,k\neq(p-1)/2,2qk^2+2qk+(p+q)/2$ 均为素数.

对于类群指数为 2 的虚二次域和一些特殊的产生素数的多项式之间的联系，Mollin 发展了更广泛的理论. 设 $d\neq 0,1$ 并且是无平方因子的负整数. Δ 是对应的基本判别式. $2\leqslant q_1<q_2<$

$\cdots < q_{N+1} = p$ 是 Δ 的全部素因子，$q = \prod_{i=1}^{N} q_i$, 对满足 $m \mid q$ 的每个正整数 m, 定义多项式

$$f_{\Delta,m}(X) = \begin{cases} mX^2 - \frac{\Delta}{4m}, & 4m \mid \Delta \\ mX^2 + mX + \frac{m^2-\Delta}{4m}, & 4m \nmid \Delta. \end{cases}$$

(注意对后一情形，$4m \mid m^2 - \Delta$). 记 $B_{\Delta,m} = [|\Delta|/4m]$. 对于 $n = \prod_{i=1}^{k} p_i^{e_i}$(其中 p_i 是不同的素数), 记 $\nu(n) = \sum_{i=1}^{k} e_i$. 又令

$$\Omega(f_{\Delta,m}(X)) = \max\left\{\nu(f_{\Delta,m}(k)) \mid 0 \leqslant k \leqslant B_{\Delta,m} - 1\right\}$$

Mollin 证明了 (见他 1996 年的书或 1997 年的综述文章)：设 $\Delta < -4$ 并利用上述记号，则下列三个命题是等价的.

(1) $e_d \leqslant 2$.

(2) $h_d = 2^N$, 并且对 q 的每个正因子 m,$\Omega(f_{\Delta,m}(X)) + \nu(m) - 1 = N$.

(3) $h_d = 2^N$, 并且存在 q 的正因子 m, 使得 $\Omega(f_{\Delta,m}(X)) + \nu(m) - 1 = N$.

取 $m = q$, 可知对于 $k = 0, 1, \cdots, B_{\Delta,q} - 1$,$f_{\Delta,q}(k)$ 均是素数. 不难验证，上述 Rabinowitsch 和 Louboutin 的早期结果均为它的特殊情形.

1986 年，Sasaki 证明了：$h_d = 2$ 当且仅当 $\Omega(f_{\Delta,1}(X)) = 2$. 这个结果也可由 Mollin 1996 年的那个定理推出.

容易看出, 前面提到的那些多项式产生素数的结果均可由 Mollin 的定理推出: $d = -2 \times 29, \Delta = -8 \times 29, N = 1$；$-d$ 为宜数，于是 $e_d \leqslant 2, m = 2, \nu(m) = 1, B_{\Delta,m} = 29, f_{\Delta,m} = 2X^2 + 29$, 从而 $\Omega(2X^2 + 29) = 1$. 所以当 $k = 0, 1, \cdots, 28$ 时，$f_{\Delta,m}$ 均为素数.

希望你能用同样的方法解释多项式 $3X^2 + 3X + 23$ 和 $6X^2 + 6X + 31$ 产生素数的性状.

到此为止，我只谈到负判别式情形，但是对于正判别式的多项式也有类似的理论．可见 Louboutin(1990), Mollin(1996,1996a) 和 Sasaki(1986a) 的文章．还有些产生素数的二次多项式没有根据任何理论，而是通过计算机寻找的．

记录

R.Ruby 于 1990 年发现，二次多项式 $f(X)=36X^2-810X+2753$ 对于 $k=0,1,\cdots,44,|f(k)|$ 均为素数，这是目前素数生成长度最大的二次多项式．

多项式 $103X^2-3945X+34381$ 和 $47X^2-1701X+10181$ 的素数生成长度均为 43, 是由 R.Ruby 和 G.Fung 分别发现的．

关于高次多项式， Dress 和 Landreau(2003) 发现 $f(X)=66X^3+83X^2-13735X+30139$ 对于连续 46 个 k 值 $(-26\sim 19)$,$|f(k)|$ 均为素数．而 $f(X)=16X^4+28X^3-1685X^2-23807X+110647$ 对于从 -23 到 22 的 k 值， $|f(k)|$ 均为素数．

如果多项式 $f(X)$ 的系数可为有理数，但是 $f(k)$ 永远为整数，则记录为

$$f(X)=\frac{1}{4}X^5+\frac{1}{2}X^4-\frac{345}{4}X^3+\frac{879}{2}X^2+17500X+70123$$

对于从 -27 到 29 的 k 值， $|f(k)|$ 均为素数．这个记录也是 Dress 和 Landreau 在预印本中给出的，很难打破这个记录．

3.3D 素数值和素因子的比赛

素数值的比赛

下面一个研究课题引起许多数学爱好者的兴趣．设 $f(X)$ 是不为常数的整系数多项式， $N\geqslant 1$. 令

$$\pi^*_{f(X)}(N)=\#\{n\mid 0\leqslant n\leqslant N,|f(n)|\text{为素数}\}$$

这里我们不要求 $|f(n)|$ 的素数值是不同的.

给了 N(通常很大) 和 $d \geqslant 1$, 我们的问题是: 决定 d 次多项式 $f(X)$, 使 $\pi^*_{f(X)}(N)$ 达到最大值. 这个问题也可限制 $f(X)$ 是首 1(即最高次项系数为 1) 多项式, 或者是某种特殊类型的首 1 多项式.

下面是一些颇有争议的记录

记录

(1) 数学家 S.M.Williams(在 1993 年 10 月的信中) 指出: 对于 $N = 1000$, 二次多项式 $f(X) = 2X^2 - 1584X + 98621$ 给出素数的最多个数, 即 $\pi^*_{f(X)}(1000) = 706$. 在此之前的记录也是 Williams 给出的. 对于

$$f_1(X) = 2X^2 - 1904X + 42403$$
$$f_2(X) = 2X^2 - 1800X - 5749$$

分别有 $\pi^*_{f_1(X)}(1000) = 693$ 和 $\pi^*_{f_2(X)}(1000) = 686$.

(2) 对于 $N = 1000$ 和二次首 1 多项式情形, 目前的冠军为

$$g(X) = (X - 499)^2 + (X - 499) + 27941$$

对此有 $\pi^*_{g(X)}(1000) = 669$, 这是由 N.Boston 发现的 (私人通信).

对于 $h(X) = X^2 + X + 27941$, 则在集合 $\{h(k) \mid 0 \leqslant k \leqslant 1000\}$ 当中有 600 个不同的素数, 这也可能是一个记录. 但这是对于规则稍有变动的比赛, 即考虑二次多项式不同的素数取值个数 (N 仍取为 1000).

1973 年, Karst 对于多项式 $f(X) = 2X^2 - 199$ 得到 597 个素数取值. 另一方面, 欧拉的多项式 $f(X) = X^2 + X + 41$ 给出 582

个素数取值. 对于这两个著名的多项式, 比赛扩大到更大的上界 N. 喜欢计算的 S.S.Gupta 在 1998 年 12 月告诉我下面的结果:

$$\pi^*_{2X^2-199}(10^7) = 2381779$$

$$\pi^*_{x^2+X+41}(10^7) = 2208197$$

我在第六章 6.4 节对于多项式 $f(X) = X^2 + X + A$ 还要考虑这个问题, 它和 Hardy-Littlewood 的一个猜想有关.

78 岁的 M.L.Greenwood 不用计算机发现多项式

$$h_1(X) = -4X^2 + 381X - 8524$$

$$h_2(X) = -2X^2 + 185X - 31819$$

当 $k = 0, 1, \cdots, 99$ 时取值有 50 个偶数和 48 个不同的奇素数. 业余爱好者 Greenwood 和 Boston 教授一起, 在 1995 年利用计算机计算了多项式 $f(X) = 41X^2 - 4641X + 88007$. 对于 $k = 0, 1, \cdots, 99$ 共取 90 个不同的素数值 $f(k)$.

现在谈高次多项式. 对于三次多项式, 取 $N = 500$(对比于 Indianapolis 的 500 英里赛车),Goetgheluck (1989) 作了研究, 获胜者为

$$f(X) = 2X^3 - 489X^2 + 39847X - 1084553$$

对 $k \leqslant 500$ 它取 267 个素数值. 在这个比赛中, 多项式的最高项系数为 1 或者 2, 并且对于其他系数的大小加上了其他限制.

今后在第六章 6.3 节, 我还要考虑相反方向的问题, 即当自变量从 $0, 1, 2, \cdots$ 到某个大数 N 时, 多项式取值为合成数的情况.

最小素因子的比赛

对于每个非零整数 m, 以 $P_0[m]$ 表示 m 的最小素因子. 如果

$f(X)=aX^2+bX+c$ 是整系数多项式， $a \geqslant 1, c \neq 0$. 令

$$P_0[f(X)]=\min\{P_0[f(k)] \mid k=0,1,2,\cdots\}$$

又对 $N \geqslant 1$, 令

$$q_N=\min\{P_0[f(k)] \mid k=0,1,2,\cdots,N\}$$

由于 $q_1 \geqslant q_2 \geqslant \cdots$ 可知存在 N 使得 $q_N < N$. 这时 $P_0[f(X)]=q_N$, 这给出计算 $P_0[f(X)]$ 的容易方式.

关于 $P_0[f(X)]=q_N$ 的证明：如果 p 为素数， $p<q_N$, 并且对某个 $M>N$ 使得 $p \mid f(M)$, 则 $M=dp+r, 0 \leqslant r<p<q_N<N$. 由 $f(M) \equiv f(r) (\bmod\ p)$ 可知 $p \mid f(r)$. 于是 $p \geqslant q_N$, 这导致矛盾.

现在令 $f_A(X)=X^2+X+A\ (A \geqslant 1)$. 已经证明了：对每个素数 q, 均存在 $A<q$, 使得 $P_0[f_A(X)]=q$. 比赛的是求 $P_0[f_A(X)]$ 的最大值. 我们有 $P_0[f_{41}(X)]=41$.

记录

若假定 A 为素数，并且求对给定 q, 求满足 $P_0[f_A(X)]=q$ 的最小素数 A, 则有

$$P_0[X^2+X+33239521957671707]=257$$

这是 P.Carmody 于 2001 年发现的. 在这之前，L.Rodríguez Torres 分别于 1996 和 1995 年给出记录

$$P_0[X^2+X+67374467]=107$$
$$P_0[X^2+X+32188691]=71$$

若 A 为素数但不必要求是最小，则 M. J. Jacobson 和 H. C. Williams 在 2002 年用一种特殊的电子筛法 (见他们 2003 年文章) 得到目前最大的 $P_0[f_A(X)]$：

对于 57 位的

$$A = 6050692910838024074222817858161664766242877869465875\allowbreak 07887$$

他们发现 $P_0[f_A(X)] = 373$.

若不要求 A 为素数，他们对于 68 位的

$$A = 473921325459343683034392483938729326577582359834725843\allowbreak 57825592740917$$

(它是 6 个素数的乘积) 给出 $P_0[f_A(X)] = 401$. 而在这之前的记录是 Patterson 和 Williams(1995) 通过长时间计算给出的

$$P_0[X^2 + X + 2457080965043150051] = 281$$

3.4 满足条件 (c) 的函数

让我们回忆一下：条件 (c) 是要求函数的全部正值构成的集合恰好为全部素数组成的集合. 令人惊奇的是，这是可能的，并且它是作为希尔伯特第十问题的副产品被发现的. 思想来源于逻辑，而结果是超常的，即使到现在它们也没有找到直接的实际应用.

我不打算介绍其技术细节，因为这些细节离素数理论太远. 所以我更多地依赖直觉和读者的善解. 请不要过于追究我所写的东西！若想深究下面的结果，建议读者去看 Davis(1973) 精彩的文章.

希尔伯特第十问题是关于不定方程 $P(X_1, \cdots, X_n) = 0$ 整数解 $(x_1, \cdots, x_n)$ 的问题，其中 P 是任意多变量的整系数多项式.

更确切地说：是否存在一个算法，它可对任意不定方程都能告诉你是否有整数解.

一个算法应当是一个确定性的程序，它可以用计算机程序来实现，经过有限步连续运算之后，可回答“是”或者“否”. 这类操作被数学家认为是合法的.

在研究一些正整数组 $(x_1,\cdots,x_n)$ 构成的集合 S 时，有以下的一个中心概念：S 叫作丢番图集合，是指存在一个以 $X_1,\cdots,X_n$, $Y_1,\cdots,Y_m$ $(m\geqslant 0)$ 为变量的整系数多项式 P, 使得 $(x_1,\cdots,x_n)\in S$ 当且仅当存在正整数 $y_1,\cdots,y_m$ 使得

$$P(x_1,\cdots,x_n,y_1,\cdots,y_m)=0$$

首先给出一个平凡的例子. 每个正整数 n 元组的有限集合是丢番图集合. 因为设 S 由 $(a_1^{(i)},\cdots,a_n^{(i)})$ $(1\leqslant i\leqslant k)$ 组成 $(k\geqslant 1)$, 令 $Y_j^{(i)}(1\leqslant i\leqslant k, 1\leqslant j\leqslant n)$ 是不同的变量，令

$$P=\prod_{i=1}^{k}\left[(X_1-Y_1^{(i)})^2+\cdots+(X_n-Y_n^{(i)})^2\right]$$

当取 $Y_j^{(i)}$ 为 $a_j^{(i)}$ 时 (对所有 i,j), 则 $(x_1,\cdots,x_n)\in S$ 当且仅当

$$P(x_1,\cdots,x_n,a_1^{(1)},\cdots,a_n^{(1)},\cdots,a_1^{(k)},\cdots,a_n^{(k)})=0$$

另一个例子：设 S 为所有正的合成数构成的集合，它也是丢番图集合. 因为 x 是正的合成数当且仅当存在正整数 y,z, 使得 (x,y,z) 为 $X-(Y+1)(Z+1)=0$ 的解.

下列事实是 Putnam 于 1960 年给出的，证明并不困难.

一个正整数集合 S 是丢番图集合，当且仅当存在一个整系数多项式 Q(变量个数 $m\geqslant 1$), 使得

$$S=\{Q(x_1,\cdots,x_m)\geqslant 1\mid x_1,\cdots,x_m\geqslant 1\}$$

这个理论的下一步是要证明素数集合为丢番图集合. 为此，需要从丢番图集合理论的角度来考察素数的定义.

正整数 x 是一个素数，当且仅当 $x > 1$, 并且对任意正整数 y 和 z, 如果 $y \leqslant x, z \leqslant x$, 那么 $yz < x, yz > x, y = 1, z = 1$ 这四者之间至少有一个成立. 在素数的这个定义中，由于 $y \leqslant x, z \leqslant x$, 可知 y 和 z 只考虑有限多个可能.

下面是素数的另一个可能的定义. 正整数 x 为素数，当且仅当 $x > 1$, 并且 $\gcd((x-1)!, x) = 1$. 后一个条件可重述为：存在正整数 a 和 b, 使得 $a(x-1)! - bx = 1$. 注意若 a 或 b 为负整数，可取充分大的整数 k', 则 $a' = a + k'x > 0, b' = b + k'(x-1)! > 0$, 仍有 $a'(x-1)! - b'x = 1$.

利用上面对于素数的任一种刻画方式，由 Putnam, Davis, J. Robinson 和 Matijasevič 发展的理论可得到下面重要的结果：

素数是丢番图集合.

这些结果合在一起，就给出下面令人惊讶的结果：

存在一个整系数多项式，使得当所有变量过全部非负整数的时候，该多项式的正值集合恰好是全部素数组成的集合.

注意此多项式也会取负值，并且某个素数作为多项式取值也可能重复出现.

1971 年， Matijasevič 给出一个代数关系集合，并由此得出：存在 (但没有明确给出) 一个 37 次和 24 个变量的多项式满足上述要求. 在他的文章的英译本中，结果改进成 21 次和 21 个变量的多项式.

1976 年， Jones,Sato,Wada 和 Wiens 给出具有此性质的一个 25 次和 26 变量 $a, b, \cdots, z$ 的多项式

$$(k+2)\{1 - [wz + h + j - q]^2 - [(gk + 2g + k + 1)(h + j) + h - z]^2$$

$$
\begin{aligned}
&-[2n+p+q+z-e]^2-[16(k+1)^3(k+2)(n+1)^2+1-f^2]^2\\
&-[e^3(e+2)(a+1)^2+1-o^2]^2-[(a^2-1)y^2+1-x^2]^2\\
&-[16r^2y^4(a^2-1)+1-u^2]^2-[((a+u^2(u^2-a))^2-1)(n+4dy)^2\\
&+1-(x+cu)^2]^2-[n+l+v-y]^2\\
&-[(a^2-1)l^2+1-m^2]^2-[ai+k+1-l-i]^2\\
&-[p+l(a-n-1)+b(2an+2a-n^2-2n-2)-m]^2\\
&-[q+y(a-p-1)+s(2ap+2a-p^2-2p-2)-x]^2\\
&-[z+pl(a-p)+t(2ap-p^2-1)-pm]^2\}
\end{aligned}
$$

人们显然试图降低变量个数 n 或者次数 d, 或者同时降低两者. 但这是要花代价的. 如果降低变量数 n, 则次数 d 便增大. 反之, 若次数 d 变小, 则 n 必须增大.

可以从表示素数多项式的表 3.1 中看到这些现象.

表 3.1　表示全部素数的多项式

n = 变量数	d = 次数	作者	时间	注记
24	37	Matijasevič	1971	未明显写出
21	21	同上	1971	
26	25	Jones, Sato Wata & Wiens	1976	第一次明显 写出多项式
42	5	同上	1976	次数最小, 未明显写出
12	13679	Matijasevič	1976	
10	约 1.6×10^{45}	同上	1977	变量数最少, 未明显写出

目前不知道这种多项式的最小可能的变量个数是多少 (肯定不能为 2). 但是 Jones 证明了这个最小值不超过 5.

研究素数集合的这种方法同样可用于其他丢番图集合, 所需

要的只是以适当的观点来描述该集合的定义中那些算术性质.

Jones 对此作了许多事情. 他在 1975 年的一篇文章中证明了斐波那契数集合是二元 5 次多项式

$$2xy^4 + x^2y^3 - 2x^3y^2 - y^5 - x^4y + 2y$$

在非负整数处的全部正值集合. 1979 年他证明了: Mersenne 素数集、偶完全数集、费马素数集, 都可用同样的方法给出对应的 7 元多项式, 但是次数比较大. 他还写出对应于上述诸集合的更多低次多项式, 但是变量要多 (见表 3.2).

表 3.2 给出各种数集合的多项式

集合	变量个数	次数
斐波那契集	2	5
Mersenne 素数集	13	26
	7	914
偶完全数集	13	27
	7	915
费马素数集	14	25
	7	905

利用 Skolem 的方法 (见他 1938 年的书), 后三个集合的多项式的次数可减到 5, 但是变量个数要增至 20 左右.

对于 Mersenne 素数集合, 对应下面的 13 元 26 次多项式

$$\begin{aligned} n\{1 - [4b + 3 - n]^2 - b([2 + hn^2 - a]^2 \\ + [n^3d^3(nd + 2)(h + 1)^2 + 1 - m^2]^2 \\ + [db + d + chn^2 + g(4a - 5) - kn]^2 \end{aligned}$$

$$\begin{aligned} &+ [(a^2 - 1)c^2 + 1 - k^2n^2]^2 + [4(a^2 - 1)i^2c^4 + 1 - f^2]^2 \\ &+ [(kn + lf)^2 - ((a + f^2(f^2 - a))^2 - 1)(b + 1 + 2jc)^2 - 1]^2)\} \end{aligned}$$

对于偶完全数集合，对应下面的 13 元 27 次多项式

$$
\begin{aligned}
&(2b+2)n\{1-[4b+3-n]^2-b([2+hn^2-a]^2\\
&\quad+[n^3d^3(nd+2)(h+1)^2+1-m^2]^2\\
&\quad+[db+d+chn^2+g(4a-5)-kn]^2\\
&\quad+[(a^2-1)c^2+1-k^2n^2]^2+[4(a^2-1)i^2c^4+1-f^2]^2\\
&\quad+[(kn+lf)^2-((a+f^2(f^2-a))^2-1)(b+1+2jc)^2-1]^2)\}
\end{aligned}
$$

对于费马素数集合，对应下面的 14 元 25 次多项式

$$
\begin{aligned}
&(6g+5)\{1-[bh+(a-12)c+n(24a-145)-d]^2\\
&\quad-[16b^3h^3(bh+1)(a+1)^2+1-m^2]^2\\
&\quad-[3g+2-b]^2-[2be+e-bh-1]^2-[k+b-c]^2\\
&\quad-[(a^2-1)c^2+1-d^2]^2-[4(a^2-1)i^2c^4+1-f^2]^2\\
&\quad-[(d+lf)^2-((a+f^2(f^2-a))^2-1)(b+2jc)^2-1]^2\}
\end{aligned}
$$

第四章　素数是如何分布的？

我曾经强调过，关于“素数有无穷多个”有许多证明．但是这些证明都是非构造性的，没有指出如何决定第 n 个素数．这也相当于说，这些证明没有告诉我们，不超过任一给定数 N 的素数有多少个．所以没有一个适宜的公式或者函数来表示全体素数．

但是，我们可以用相当好的准确度来预测 N 以内素数的个数(特别当 N 很大的时候)．另一方面，素数在一些短区间内的分布是相当没有规律的．这种既“随机”又“可预测”相组合便使得素数的分布既是有序的排列，同时又有意外的现象． Schroeder 在他精彩的书《科学和通信中的数论》(1984) 一书中，把这种现象称作是艺术作品的基本要素．许多数学家都认为素数分布问题具有极大的美学动力．

在第三章中，对每个实数 $x > 0$，以 $\pi(x)$ 表示不超过 x 的素数个数，叫作 **素数计算函数**．

我们要考虑以下事情：

(1) $\pi(x)$ 的性质：增长情况，函数的数量级，与其他已知函数加以比较．

(2) 关于第 n 个素数：相邻素数之差能有多小，能有多大，怎样地没有规律．其中包括相邻素数的最大间隙，从而产生以下的一些未解问题．

(3) 孪生素数问题，如何刻画它们，它们的分布．

(4) k- 素数组问题．

(5) 算术级数中的素数．

(6) 哥德巴赫著名猜想.

(7) 拟素数和 Carmichael 数的分布.

现在我讨论这些问题.

4.1 函数 $\pi(x)$

研究函数 $\pi(x)$ 或者与素数分布有关的其他问题, 其基本思想是与一些经典并且可计算的函数加以比较, 使得这些函数的取值与 $\pi(x)$ 尽可能接近. 问题当然不是那么简单, 误差总是存在的. 所以对每个逼近函数, 需要估计相差函数 (即误差项) 的数量级. 自然地引入以下一些记号.

设 $f(x), h(x)$ 为定义于 $x \geqslant x_0 > 0$ 中取值正实数的连续函数. 记号 $f(x) \sim h(x)$ 表示 $\lim\limits_{x\to\infty} f(x)/h(x) = 1$. 这时称 $f(x)$ 和 $h(x)$**渐近地相等** (当 x 趋于无穷时). 注意它们的差也可能趋于无穷.

在上述假设之下, 如果存在常数 C 和 $C', 0 < C < C'$ 和 $x_0, x_1, x_1 \geqslant x_0$, 使得对所有 $x \geqslant x_1$, 均有 $C \leqslant f(x)/h(x) \leqslant C'$, 则称 $f(x)$ 和 $h(x)$ 有 **相同的数量级**.

若 $f(x), g(x), h(x)$ 都是 $x \geqslant x_0 > 0$ 中的实值连续函数, 并且当 $x \geqslant x_0$ 时 $h(x) > 0$. 记号

$$f(x) = g(x) + O(h(x))$$

表示存在常数 $C > 0$ 和 $x_1 \geqslant x_0$, 使得当 $x \geqslant x_1$ 时 $|f(x) - g(x)| \leqslant Ch(x)$ 成立. 当 $f(x)$ 用 $g(x)$ 代替时, 这是表示误差大小的有益记号. 类似地, 记号

$$f(x) = g(x) + o(h(x))$$

表示 $\lim\limits_{x\to\infty}[f(x) - g(x)]/h(x) = 0$. 形象地说, 误差与 $h(x)$ 相比较

可以忽略不计.

4.1A 历史的展现

一个适宜的方式是以历史的顺序来描述在素数定理的研究中所积累的关于素数分布的各种发现. Landau 在他著名的著作《素数分布讲义》(Handbuch der Lehre von der Verteilung der Primzahlen) 中讲述素数分布经典工作时就是这样做的. 在 Landau 之前, Torelli (1901) 用意大利文写的长篇文章, 也是以历史为线索讲述素数.

欧拉

我首先给出欧拉的一个结果. 这个结果说: 素数不仅有无穷多个, 而且“素数不像平方数那样稀疏”. (马上就要讲它的确切意思.)

欧拉注意到级数 $\sum\limits_{n=1}^{\infty} n^{-\sigma}$ 对于每个实数 $\sigma > 1$ 都是收敛的. 事实上对每个 $\sigma_0 > 1$, 它在半直线 $\sigma_0 \leqslant x < \infty$ 上是一致收敛的. 所以对 $1 < \sigma < \infty$ 它定义了一个连续可微函数 $\zeta(\sigma)$. 进而, $\lim\limits_{\sigma \to \infty} \zeta(\sigma) = 1$, $\lim\limits_{\sigma \to 1+0} (\sigma - 1)\zeta(\sigma) = 1$. 函数 $\zeta(\sigma)$ 叫作 **zeta 函数**.

zeta 函数和素数之间的联系就是下面的欧拉乘积公式, 它相当于整数表示成素数乘积的唯一分解性

$$\sum_{n=1}^{\infty} \frac{1}{n^{\sigma}} = \prod_{p} \frac{1}{1 - \frac{1}{p^{\sigma}}} \quad (\sigma > 1)$$

特别地, 当 $\sigma > 1$ 时 $\zeta(\sigma) \neq 0$.

欧拉由此证明了素数有无穷多个 (见第一章). 用同样的思想欧拉于 1737 年证明了

素数倒数之和是发散的: $\sum\limits_{p} (1/p) = \infty$.

证明 设 N 为任意自然数, 每个整数 $n < N$ 均唯一表示成

素数 p 方幂的乘积，其中 $p \leqslant n \leqslant N$. 而对每个素数 p

$$\sum_{k=0}^{\infty} \frac{1}{p^k} = \frac{1}{1-\dfrac{1}{p}}$$

于是

$$\sum_{n=1}^{N} \frac{1}{n} \leqslant \prod_{p \leqslant N} \left(\sum_{k=0}^{\infty} \frac{1}{p^k} \right) = \prod_{p \leqslant N} \frac{1}{1-\dfrac{1}{p}}$$

但是

$$\lg \prod_{p \leqslant N} \frac{1}{1-\frac{1}{p}} = -\sum_{p \leqslant N} \lg \left(1-\frac{1}{p}\right)$$

而对每个素数 p

$$\begin{aligned} -\lg\left(1-\frac{1}{p}\right) &= \sum_{m=1}^{\infty} \frac{1}{mp^m} \leqslant \frac{1}{p} + \frac{1}{p^2}\left(\sum_{h=0}^{\infty} \frac{1}{p^h}\right) \\ &= \frac{1}{p} + \frac{1}{p^2} \times \frac{1}{1-\frac{1}{p}} = \frac{1}{p} + \frac{1}{p(p-1)} \\ &< \frac{1}{p} + \frac{1}{(p-1)^2} \end{aligned}$$

因此

$$\begin{aligned} \lg \sum_{n=1}^{N} \frac{1}{n} &\leqslant \lg \prod_{p \leqslant N} \frac{1}{1-\frac{1}{p}} \leqslant \sum_{p \leqslant N} \frac{1}{p} + \sum_{p \leqslant N} \frac{1}{(p-1)^2} \\ &\leqslant \sum_{p} \frac{1}{p} + \sum_{n=1}^{\infty} \frac{1}{n^2} \end{aligned}$$

而级数 $\sum\limits_{n=1}^{\infty}(1/n^2)$ 是收敛的. 由于 N 可以为任意大而调和级数是发散的，所以 $\lg \sum\limits_{n=1}^{\infty} 1/n = \infty$, 从而级数 $\sum\limits_{p}(1/p)$ 发散. □

我已经说过级数 $\sum\limits_{n=1}^{\infty}(1/n^2)$ 是收敛的. 所以我们可以粗略地说，素数不像平方数那样稀疏.

欧拉最漂亮的发现之一是算出了

$$\sum_{n=1}^{\infty}\frac{1}{n^2}=\frac{\pi^2}{6}$$

对每个 $k\geqslant 1$ 欧拉也计算出 $\sum\limits_{n=1}^{\infty}n^{-2k}$, 从而解决了一个相当困难的问题. 为此他利用了伯努利数，定义为

$$B_0=1,\qquad B_1=-\frac{1}{2},\qquad B_2=\frac{1}{6},\cdots$$

而一般的 B_k 用下面关系递归地得出

$$\binom{k+1}{1}B_k+\binom{k+1}{2}B_{k-1}+\cdots+\binom{k+1}{k}B_1+B_0=0$$

这些数都是有理数. 容易看出对每个 $k\geqslant 1, B_{2k+1}=0$. 这些数是下列泰勒展开式中的系数

$$\frac{x}{e^x-1}=\sum_{k=0}^{\infty}\frac{B_k}{k!}x^k$$

利用 Stirling 公式

$$n!\sim\frac{\sqrt{2\pi}n^{n+1/2}}{e^n}\quad(n\to\infty)$$

可以证明

$$|B_{2n}|\sim 4\sqrt{\pi n}\left(\frac{n}{\pi\mathrm{e}}\right)^{2n}$$

所以上面的级数在 $|x|<2\pi$ 时收敛.

欧拉用伯努利数表达和式

$$\sum_{j=1}^{n}j^k=S_k(n)\quad(k\geqslant 1)$$

其中

$$
\begin{aligned}
S_k(X) = & \frac{1}{k+1}\left[X^{k+1} - \binom{k+1}{1}B_1X^k + \binom{k+1}{2}B_2X^{k-1}\right. \\
& \left. + \cdots + \binom{k+1}{k}B_kX\right]
\end{aligned}
$$

大约同一时间，日本人 Seki 也得到类似的表达式.

关于 $\zeta(2k)$ 的欧拉公式为

$$\zeta(2k) = \sum_{n=1}^{\infty}\frac{1}{n^{2k}} = (-1)^{k+1}\frac{(2\pi)^{2k}B_{2k}}{2(2k)!}$$

特别地

$$
\begin{aligned}
\zeta(2) &= \sum_{n=1}^{\infty}\frac{1}{n^2} = \frac{\pi^2}{6} \quad \text{(已经提到过)} \\
\zeta(4) &= \sum_{n=1}^{\infty}\frac{1}{n^4} = \frac{\pi^2}{90} \\
&\vdots
\end{aligned}
$$

欧拉还考虑如下定义的伯努利多项式

$$B_k(X) = \sum_{i=0}^{k}\binom{k}{i}B_iX^{k-i} \qquad (k \geqslant 0)$$

这些多项式可以用来重新写出 $S_k(X)$ 的表达式，但是最重要的应用是将通常的阿贝尔求和公式极大地推广为下面著名的欧拉 - 麦克劳林求和公式.

如果 $f(x)$ 是无限次连续可微函数， a 和 b 均为整数， $a < b$,

则对每个 $k \geqslant 1$

$$\sum_{n=a+1}^{b} f(n) = \int_a^b f(t)\mathrm{d}t + \sum_{r=1}^{k}(-1)^r \frac{B_r}{r!}\{f^{(r-1)}(b) - f^{(r-1)}(a)\}$$
$$+ \frac{(-1)^{k-1}}{k!}\int_a^b B_k(t-[t])f^{(k)}(t)\mathrm{d}t$$

(我们已经解释过，$[t]$ 表示 t 的整数部分).

建议读者去看 Ayoub 的文章“欧拉和 zeta 函数” (Euler and the zeta function 1974). 在这篇文章中介绍了关于 $\zeta(s)$ 的许多想像中的关系式和欧拉的许多发现，其中有些事情是完全被证明了的，另一些关系只是很好玩. 这些结果均先于黎曼的工作.

勒让德

勒让德 (1808) 第一个尝试对函数 $\pi(x)$ 认真地加以研究，他用 Eratosthenes 筛法证明了

$$\pi(N) = \pi(\sqrt{N}) - 1 + \sum \mu(d)\left[\frac{N}{d}\right]$$

其中求和 d 过所有正整数，并且 d 的素因子均不超过 $\sqrt{N}$，而 Möbius 函数 $\mu(n)$ 已在第三章 3.1 节给出定义.

作为这个公式的一个推论，勒让德证明了 $\lim\limits_{x\to\infty}(\pi(x)/x) = 0$，但这是一个相当弱的结果. 通过计算实验，勒让德于 1798 年 (后来又在 1808 年) 猜想

$$\pi(x) = \frac{x}{\lg x - A(x)}$$

其中 $\lim\limits_{x\to\infty} A(x) = 1.08366\cdots$. 四十年后切比雪夫 (见后面) 证明了：若 $\lim\limits_{x\to\infty} A(x)$ 存在，它必须等于 1.Pintz(1980) 给出一个简单的证明.

高斯

高斯 15 岁的时候 (1792 年) 猜想： $\pi(x)$ 和函数

$$\mathrm{L}i(x)=\int_2^x \frac{\mathrm{d}t}{\lg t}$$

渐近地相等. 由于 $\mathrm{L}i(x)\sim x/\lg x$, 所以这相当于

$$\pi(x)\sim \frac{x}{\lg x}$$

这也曾由勒让德不十分明确地猜想过. 这个猜想后来被肯定，就是现在熟知的素数定理，我马上就会讲到它.

$\pi(x)$ 用 $x/\lg x$ 作为近似在理论上比较好，但是正如表 4.1 所显示的，采用对数积分逼近程度要好得多.

表 4.1　$\pi(x)$的值并与 $x/\lg x, Li(x), R(x)$比较

x	$\pi(x)$	$(x/\lg x)-\pi(x)$	$Li(x)-\pi(x)$	$R(x)-\pi(x)$
10^8	5761455	−332774	754	97
10^9	50847534	−2592592	1701	−79
10^{10}	455052511	−20758030	3104	−1828
10^{11}	4118054813	−169923160	11588	−2318
10^{12}	37607912018	−1416705193	38263	−1476
10^{13}	346065536839	−11992858452	108971	−5773
10^{14}	3204941750802	−102838308636	314890	−19200
10^{15}	29844570422669	−891604962453	1052619	73218
10^{16}	279238341033925	−7804289844393	3214632	327052
10^{17}	2623557157654233	−68883734693929	7956589	−598255
10^{18}	24739954287740860	−612483070893537	21949555	−3501366
10^{19}	234057667276344607	−5481624169369961	99877775	23884333
10^{20}	2220819602560918840	−49347193044659702	222744643	−4891825
10^{21}	21127269486018731928	−446579871578168707	597394254	−86432204

切比雪夫(Tschebycheff)

关于 $\pi(x)$ 的数量级的重大进展是由切比雪夫于 1850 年给出的. 他利用初等方法证明了：对每个 $\varepsilon>0$ 都存在 $x_0>0$, 使得当 $x>x_0$ 时

$$(C'-\varepsilon)\frac{x}{\lg x}<\pi(x)<(C+\varepsilon)\frac{x}{\lg x}$$

其中

$$C' = \lg \frac{2^{1/2}3^{1/3}5^{1/5}}{30^{1/30}} = 0.92129\cdots, \quad C = \frac{6}{5}C' = 1.10555\cdots$$

进而，切比雪夫证明了：若极限

$$\frac{\pi(x)}{x/\lg x}$$

存在 (当 $x \to \infty$ 时), 它一定为 1. 他还推导出勒让德关于 $\pi(x)$ 的近似值推断中的 1.08366 应当为 1(见 Landau 的书，第 17 页).

切比雪夫还证明了 Bertrand 猜测：对于任何自然数 $n \geqslant 2$, 在 n 和 $2n$ 之间至少有一个素数. 我在讲述函数 $\pi(x)$ 的主要性质时还会讨论这个结论.

切比雪夫研究函数 $\theta(x) = \sum\limits_{p \leqslant x} \lg p$, 现在它叫作切比雪夫函数，它基本上给出和 $\pi(x)$ 同样的信息，但是比较容易研究.

切比雪夫已经十分接近于证明高斯所猜想的素数定理，但还需等了大约五十年，在 19 世纪末期才被证明. 在这段时期黎曼贡献了重要的新思想.

黎曼(Riemann)

黎曼的思想是把 zeta 函数定义在实数部分大于 1 的复数 s 上，即

$$\zeta(s) = \sum_{n=1}^{\infty} n^{-s}$$

对每个 $\mathrm{Re}(s) > 1$ 的复数 s, 欧拉乘积公式仍旧成立. 利用欧拉 - 麦克劳林求和公式， $\zeta(s)$ 可以表达成

$$\zeta(s) = \frac{1}{s-1} + \frac{1}{2} + \sum_{r=2}^{k} \frac{B_r}{r!} s(s+1)\cdots(s+r-2)$$

$$-\frac{1}{k!}s(s+1)\cdots(s+k-1)\int_1^\infty B_k(x-[x])\frac{\mathrm{d}x}{x^{s+k}}$$

其中 $k \geqslant 1$ 为任何整数，B_r 是伯努利数，请不要把它和 $B_k(x-[x])$ 混淆，后者是伯努利多项式 $B_k(X)$ 在 $x-[x]$ 处的取值.

积分在 $\mathrm{Re}(s) > 1-k$ 时收敛. 由于 k 可取任何自然数，用这个公式可把 $\zeta(s)$ 解析开拓到整个复平面上. $\zeta(s)$ 在 $s=1$ 有单极点并且留数为 1，即

$$\lim_{s\to 1}(s-1)\zeta(s) = 1$$

在 $s=1$ 之外 $\zeta(s)$ 是解析的.

1859 年黎曼建立了 zeta 函数的函数方程. 由于这个方程中有伽玛函数 $\Gamma(s)$，我先定义 $\Gamma(s)$. 对于 $\mathrm{Re}(s) > 0$，伽玛函数可方便地定义成欧拉积分

$$\Gamma(s) = \int_0^\infty e^{-u}u^{s-1}\mathrm{d}u$$

对任何复数 s，它可定义成

$$\Gamma(s) = \frac{1}{s\mathrm{e}^{\gamma s}}\prod_{n=1}^{\infty}\frac{\mathrm{e}^{s/n}}{1+s/n}$$

其中 γ 为欧拉常数

$$\gamma = \lim_{n\to\infty}\left(1+\frac{1}{2}+\cdots+\frac{1}{n}-\lg n\right) = 0.577215665\cdots$$

欧拉常数 (意大利人也称为 Mascheroni 常数) 通过下面的 Mertens 公式与欧拉乘积联系起来：

$$e^r = \lim_{n\to\infty}\frac{1}{\lg p_n}\prod_{i=1}^{n}\frac{1}{1-1/p_i}$$

$\Gamma(s)$ 没有零点，在点 $0,-1,-2,-3,\cdots$ 处为单极点，其他地方均解析. 对每个正整数 n, $\Gamma(n)=(n-1)!$ 所以伽玛函数是函数 $n!$ 的扩充. 伽玛函数满足许多有趣的关系，其中包括函数方程

$$\Gamma(s)\Gamma(1-s)=\frac{\pi}{\sin\pi s},\quad \Gamma(s+1)=s\Gamma(s)$$

和

$$\Gamma(s)\Gamma(s+1/2)=\frac{\sqrt{\pi}}{2^{2s-1}}\Gamma(2s)$$

现在可以写出黎曼 zeta 函数的函数方程

$$\pi^{-s/2}\Gamma\left(\frac{s}{2}\right)\zeta(s)=\pi^{-(1-s)/2}\Gamma\left(\frac{1-s}{2}\right)\zeta(1-s)$$

由黎曼方程可得到许多事情，如 $\zeta(0)=-1/2$.

zeta 函数的零点为：

(1) 在 $-2,-4,-6,\cdots$ 处为单零点，叫作平凡零点；

(2) 其余零点都在带状临界区域 $0\leqslant \mathrm{Re}(s)\leqslant 1$ 之中.

这是由于当 $\mathrm{Re}(s)>1$ 时，由欧拉乘积公式可知 $\zeta(s)\neq 0$. 如果 $\mathrm{Re}(s)<0$, 则 $\mathrm{Re}(1-s)>1$. 函数方程的右边没有零点，从而 $\zeta(s)$ 的零点只有 $\Gamma(s/2)$ 的极点 $s=-2,-4,-6,\cdots$

在临界区域中的零点知识对于理解素数的分布有重要影响. 首先注意到临界区域中的零点不是实数，并且关于实轴和垂直线 $\mathrm{Re}(x)=1/2$ 都是对称的.

黎曼猜想： $\zeta(s)$ 的所有非平凡零点 ρ 都在临界直线 $\mathrm{Re}(s)=1/2$ 之上, 即 $\rho=1/2+\mathrm{i}\gamma$. 这就是著名的黎曼猜想, 它至今未被证明. 它无疑是数论中，也可以说是整个数学中，一个最困难和最重要的问题. 我很快会回到这个猜想，集中讨论一些现代进展.

现在我想很粗糙地指出黎曼如何给出 $\pi(x)$ 的一个更好的逼近. 对每个实数 $x>0$, 他定义

$$J(x)=\pi(x)+\frac{1}{2}\pi(x^{1/2})+\frac{1}{3}\pi(x^{1/3})+\frac{1}{4}\pi(x^{1/4})+\cdots$$

注意在 $2^n > x$ 时，这个求和式中的项 $\pi(x^{1/n})$ 为 0, 所以对每个 x, 上面表达式都是有限项之和. 用 Möbius 反演公式得到

$$\pi(x)=\sum_{n=1}^{\infty}\frac{\mu(n)}{n}J\big(x^{1/n}\big)\quad(\text{仍是有限和})$$

黎曼工作的最本质部分是用复变量的对数积分表达 $J(x)$ 的解析公式. 令 $w=u+\mathrm{i}v$, 按照 $v>0, v<0$ 或 $v=0$, 分别定义 $z=\pi\mathrm{i}, -\pi\mathrm{i}$ 或 0. 由定义

$$Li(e^w)=\int_C\frac{\mathrm{e}^t}{t}\mathrm{d}t$$

其中 C 为水平直线， $C=\{s+\mathrm{i}v\mid -\infty<s\leqslant u\}$. 黎曼证明了函数 $J(x)$ 如下的基本解析公式:

对所有 $x>0$

$$J(x)=Li(x)-\sum_{\rho}Li(x^{\rho})-\lg 2+\int_x^{\infty}\frac{\mathrm{d}t}{t(t^2-1)\lg t}$$

其中求和过 zeta 函数在上半平面的全部非平凡零点 ρ. 将 $J(x^{1/n})$ 代到 $\pi(x)$ 的表达式中，给出 $\pi(x)$ 用对数积分的如下表达式:

$$\pi(x)=\sum_{n=1}^{\infty}\frac{\mu(n)}{n}Li(x^{1/n})+(\text{包含非平凡零点的其他项}).$$

毋庸置疑，这种分析考虑很精细，对黎曼也曾是一个挑战. 而且依赖于非平凡零点 ρ 的那些项的估计是非常困难的. 但是由实际计算显示出，黎曼函数

$$R(x)=\sum_{n=1}^{\infty}\frac{\mu(n)}{n}Li(x^{1/n})$$

给出 $\pi(x)$ 的非常好的逼近，见表 4.1.

Gram 在 1893 年给出用一个快速收敛级数计算黎曼函数的方法

$$R(x)=1+\sum_{n=1}^{\infty}\frac{1}{n\zeta(n+1)}\cdot\frac{(\lg x)^n}{n!}$$

我建议读者参考 Edwards 的书 (1974), 在书中对于素数分布的黎曼工作作了透彻的介绍. 关于黎曼 zeta 函数的书还有经典著作 Titchmarsh(1951) 和近来的书 Ivić(1985) 和 Patterson(1988).

de la Vallée Poussin 和 Hadamard

黎曼为素数基本定理

$$\pi(x)\sim\frac{x}{\lg x}$$

提供了许多工具, 另一些工具则来源于快速发展的复解析函数理论.

素数定理逐渐成为了 "最希望证明的定理", 证明这个定理的人被认为是不朽的. 它被两个杰出的分析学家在同一年 (1896) 独立地证明. 他们并不像古希腊传说那样变成是不朽的, 但也差不多如此！ Hadamard 活了 98 岁, 而 de la Vallée Poussin 只差一点, 活了 96 岁.

de la Vallée Poussin 建立了以下结果: 存在 $c>0$ 和 $t_0=t_0(c)>\mathrm{e}^{2c}$, 使得在区域

$$\begin{cases}1-c/\lg t_0\leqslant\sigma\leqslant 1, & |t|\leqslant t_0\\ 1-c/\lg|t|\leqslant\sigma\leqslant 1, & t_0\leqslant|t|\end{cases}$$

中的每个 $s=\sigma+\mathrm{i}t$ 都有 $\zeta(s)\neq 0$. 特别地推出 Hadamard 证明的一个结果, 对每个 t, $\zeta(1+\mathrm{i}t)\neq 0$.

素数定理证明的重要方面是决定 $\zeta(s)$ 一个大的无零点区域.

Hadamard 和 de la Vallée Poussin 不仅证明了素数定理，而且还估计了误差项

$$\pi(x) = Li(x) + O\left(x\mathrm{e}^{-A\sqrt{\lg x}}\right)$$

其中 A 为正的常数. 我将马上要讲到：由于 zeta 函数的无零点区域不断扩大，这个误差的估计也越来越小.

素数定理的解析证明还有不少其他方式,出现在许多书和文章中. 可见 Grosswald(1964). 一个特别简单的证明由 Newman(1980) 给出.

素数定理还有一些等价的叙述方式. 利用切比雪夫函数，素数定理可以重新叙述成

$$\theta(x) \sim x$$

另一种形式用 von Mangoldt 函数的求和. 令

$$\Lambda(n) = \begin{cases} \lg p, & n = p^{\nu}(\nu \geqslant 1), p \text{ 为素数} \\ 0, & \text{其他} \end{cases}$$

von Mangoldt 引进这个函数，与 zeta 函数的对数微商有如下关系：

$$-\frac{\zeta'(s)}{\zeta(s)} = \sum_{n=1}^{\infty} \frac{\Lambda(n)}{n^s} \quad (\text{对于} \mathrm{Re}(s) > 1)$$

这个函数与 $J(x)$ 的关系已经见到过

$$J(x) = \sum_{n \leqslant x} \frac{\Lambda(n)}{\lg n}$$

而 $\Lambda(n)$ 的求和函数定义为

$$\psi(x) = \sum_{n \leqslant x} \Lambda(n)$$

它不难用切比雪夫函数表达成

$$\psi(x)=\theta(x)+\theta(x^{1/2})+\theta(x^{1/3})+\cdots$$

从而素数定理也可表示成

$$\psi(x)\sim x$$

Erdös 和 Selberg

很长一段时间里，人们一直相信在素数定理的证明中，解析方法是不可避免的．所以当 Erdös 和 Selberg 于 1949 年同时给出素数定理的初等证明时，引起数学界的惊讶．他们的证明本质上只利用了对一些算术函数的初等估计．有不少和式的估计是熟知的，例如

$$\sum_{n\leqslant x}\frac{1}{n}=\lg x+\gamma+O\left(\frac{1}{x}\right)\quad(\gamma\text{为欧拉常数})$$

$$\sum_{n\leqslant x}\frac{1}{n^\sigma}=\frac{x^{1-\sigma}}{1-\sigma}+\zeta(\sigma)+O\left(\frac{1}{x^\sigma}\right),\quad(\sigma>1)$$

$$\sum_{n\leqslant x}\lg n=x\lg x-x+O(\lg x)$$

$$\sum_{n\leqslant x}\frac{\lg n}{n}=\frac{1}{2}(\lg x)^2+\mathrm{C}+O\left(\frac{\lg x}{x}\right)$$

这些估计可用阿贝尔或欧拉 - 麦克劳林求和公式推出，不依赖于函数的算术意义．下面是包含素数的一些更有趣的求和估计：

$$\sum_{p\leqslant x}\frac{\lg p}{p}=\lg x+O(1)$$

$$\sum_{p\leqslant x}\frac{1}{p}=\lg\lg x+C+O\left(\frac{1}{\lg x}\right),\quad C=0.2615\cdots$$

$$\sum_{n\leqslant x}\frac{\Lambda(n)}{n}=\lg x+O(1)$$

$$\sum_{n\leqslant x}\frac{\Lambda(n)\lg n}{n}=\frac{1}{2}(\lg x)^2+O(\lg x)$$

Selberg 于 1949 年得到以下估计：

$$\sum_{p\leqslant x}(\lg p)^2+\sum_{pq\leqslant x}(\lg p)(\lg q)=2x\lg x+O(x)$$

其中 p 和 q 为素数．这个估计事实上与下列公式的每个都是等价的：

$$\theta(x)\lg x+\sum_{p\leqslant x}\theta\left(\frac{x}{p}\right)\lg p=2x\lg x+O(x)$$

$$\sum_{n\leqslant x}\Lambda(n)\lg n+\sum_{mn\leqslant x}\Lambda(m)\Lambda(n)=2x\lg x+O(x)$$

Selberg 由他的这个估计式得到素数定理的初等证明．与此同时， Erdös 利用 Selberg 估计的一个类似公式

$$\frac{\psi(x)}{x}+\frac{1}{\lg x}\sum_{n\leqslant x}\frac{\psi(x/n)}{x/n}\frac{\Lambda(n)}{n}=2+O\left(\frac{1}{\lg x}\right)$$

并采用不同的初等方法也证明了素数定理．

Diamond 和 Steinig 于 1970 年给出具有明确误差项的一个初等证明． Diamond 在 1982 年的文章对于素数分布理论初等方法作了详尽和权威的介绍．

4.1B　包含 Möbius 函数的一些和式

在 Möbius 之前欧拉就曾研究过函数 $\mu(n)$．根据数值计算的显示，欧拉在 1748 年猜想 $\sum_{n=1}^{\infty}\frac{\mu(n)}{n}$ 收敛于 0.von Mangoldt 用素数定理证明了这个猜想．事实上反过来也成立，即由它也可证明素数定理．

对每个 $s, \mathrm{Re}(s) > 1$

$$\sum_{n=1}^{\infty} \frac{\mu(n)}{n^s} = \frac{1}{\zeta(s)}$$

特别当 $s = 2$ 时，由此推出对每个 $x > 1$

$$\sum_{n \leqslant x} \frac{\mu(n)}{n^2} = \frac{6}{\pi^2} + O(1/x)$$

Möbius 函数的求和函数

$$M(x) = \sum_{n \leqslant x} \mu(n)$$

叫作 Mertens 函数. 可以证明素数定理也等价于 $\lim\limits_{x\to\infty} M(x)/x = 0$. 关于上述这些论断，详见 Landau(1909),Ayoub(1963) 或者 Apostol(1976) 的书.

Daboussi 于 1984 年给出 $\lim\limits_{x\to\infty} M(x)/x = 0$ 的一个初等证明. 从而给出素数定理又一个初等证明方法，不利用 Selberg 不等式.

关于 $M(x)$ 的数量级， Mertens 本人猜想 $|M(x)| \leqslant \sqrt{x}$. 这是一个重要而困难的问题， Stieltjes 和 Hadamard 等早期数论学家都研究过这个问题. 但是 Odlyzko 和 te Riele 在 1985 年证明这个猜想是错的，因为他们证明了

$$\limsup_{x\to\infty} \frac{M(x)}{\sqrt{x}} > 1.06, \qquad \liminf_{x\to\infty} \frac{M(x)}{\sqrt{x}} < -1.009$$

Pintz 在 1987 年发表的文章中，给出此猜想错误的一个有效性证明：存在某个 $x_0, \lg x_0 < 3.21 \times 10^4$ 使得 $|M(x_0)| > \sqrt{x_0}$ [详见 te Riele(1985) 文章].

4.1C 素数表

现在回来谈素数表和数的因子分解表 (只考虑不被 2, 3 或 5 整除的数).Brancker 于 1668 年首先给出一个较大的表 (100000 以内数的最小因子),Krüger 于 1748 年列出 100000 以内的素数, Lambert 于 1770 年给出 102000 以内数的最小因子, Filkel 于 1776 年给出 408000 以内数的最小因子, Vega 于 1797 年列出 400031 以内的素数, Chernac 于 1811 年给出 1020000 以内数的素因子, Burckhardt 于 1816~1817 年给出 3036000 以内数的最小因子. 勒让德和高斯就是根据这些表中数据作了许多直觉性的观察.

这些表后来仍慢慢地扩大. 1856 年 Crelle 杂志把 6000000 以内的素数表提交给柏林科学院, 而 Dase 在 1861 年之后又把此表扩大到 9000000.

与此有关的是 Kulik 制造了 100330220 内整数 (不被 2, 3, 5 整除) 的因子表. 它花了 20 年做这个表, 在他去世 (1863 年) 之后, 这个八卷 4212 页的材料于 1867 年 2 月交给维也纳科学院.

D.N.Lehmer 于 1909 年发表了 10^7 以内数的因子表, 1914 年他发表了 10^7 以内的素数表. 这时, 这些表格被广泛地流传并为数学家们所采用.

由于计算机的进步, 许多数据表被作成磁带, 在任何大小适当的区间内, 这些数据都可用 Eratosthens 筛法快速地找到.

为了使读到此处的读者更能欣赏和使用方便, 我在文献中取出 10^4 以内的素数放在书的后面, 希望大家喜欢!

4.1D $\pi(x)$的确切值和与 $x/\lg x, Li(x), R(x)$的比较

$\pi(x)$确切值计算

$\pi(x)$ 的确切值可以从素数表中数出, 也可用 Meissel 在 1871

年设计的一个聪明的方法算出. 他用这个方法算出的结果超出素数表的范围. 用这个方法计算 $\pi(x^{1/2})$, 需要知道不超过 $x^{1/2}$ 的全部素数和 $y \leqslant x^{2/3}$ 的全部值 $\pi(y)$. 然后根据下面的公式:

$$\pi(x) = \varphi(x,m) + m(s+1) + \frac{s(s-1)}{2} - 1 - \sum_{i=1}^{s} \pi\left(\frac{x}{p_{m+i}}\right)$$

其中 $m = \pi(x^{1/3}), n = \pi(x^{1/2}), s = n - m$, 而 $\varphi(x,m)$ 表示在不超过 x 的正整数当中不被 $2, 3, \cdots, p_m$ 整除的整数个数.

当 m 很大时, $\varphi(x,m)$ 的计算需要花时间, 但这没有太大的困难, 因为计算中可利用下面一些关系:

递归关系

$$\varphi(x,m) = \varphi(x,m-1) - \varphi\left(\left[\frac{x}{p_m}\right], m-1\right)$$

除法性质

若 $P_m = p_1 p_2 \cdots p_m, a \geqslant 0, 0 \leqslant r < P_m$, 则

$$\varphi(aP_m + r, m) = a\varphi(P_m) + \varphi(r,m)$$

对称性质

若 $\frac{1}{2}P_m < r < P_m$, 则

$$\varphi(r,m) = \varphi(P_m) - \varphi(P_m - r - 1, m)$$

Meissel 于 1885 年计算了 $\pi(10^9)$(但是他算出的数小了 56).1946 年 Brauer 给出 Meissel 公式一个简单的证明. Lehmer 在 1959 年又简化和推广了 Meissel 方法. Lagarias,Miller 和 Odlyzko 采用新的筛法技术, 于 1985 年又把方法作了改进. 他们对 4×10^{16} 以内的 x 计算了 $\pi(x)$ 值. 而 Deléglise 和 Rivat(1996) 又把 x 扩大到 10^{18}. 这些

计算由 Deléglise 扩大到 $\pi(10^{20})$ (1996 年 4 月宣布), 而由 X.Gourdon 扩大到 $\pi(10^{21})$(2000 年 10 月宣布). 表 4.1 给出 x 到 10^{21} 的 $\pi(x)$ 值，并与函数 $x/\lg x, Li(x)$ 和 $R(x)$ 的对应值作了比较.

下面的值也计算出来

$$\pi(4\ 185\ 296\ 581\ 467\ 695\ 669) = 10^{17}$$

记录

X.Gourdon 和 P.Demichel 用分布式计算方法算出 $\pi(x)$ 的最大数值. 最近计算的数值为

x	$\pi(x)$	$Li(x)-\pi(x)$	$R(x)-\pi(x)$
2×10^{21}	41644391885053857293	1454564714	501830649
4×10^{21}	82103246362658124007	1200472717	−127211330
10^{22}	201467286689315906290	1932355207	−127132665
2×10^{22}	397382840070993192736	2732289619	−139131087
4×10^{22}	783964159847056303858	5101648384	1097388163

$\pi(x)$和 $x/\lg x$相比较

我已经提到过关于 $\pi(x)$ 的切比雪夫不等式，它可用初等方法证明，并且证明先于素数定理. 1892 年 Sylvester 将切比雪夫方法精细化，给出如下的明显估计:

对每个充分大的 x

$$0.95695\frac{x}{\lg x} < \pi(x) < 1.04423\frac{x}{\lg x}$$

(见 Langevin1977 年文章). 基于教学的目的， Erdös(1932) 对于较弱的不等式

$$\lg 2\frac{x}{\lg x} < \pi(x) < 2\lg 2\frac{x}{\lg x}$$

给了一个巧妙的证明. Rosser 和 Schoenfeld 通过十分精巧的分

析，于 1962 年给出估计式

$$\frac{x}{\lg x}\left(1+\frac{1}{2\lg x}\right) < \pi(x) \quad (x \geqslant 59)$$

$$\pi(x) < \frac{x}{\lg x}\left(1+\frac{3}{2\lg x}\right) \quad (x > 1)$$

Dusart 在 1998 年学位论文中把这些和文献中一些其他结果改进为

$$\frac{x}{\lg x}\left(1+\frac{1}{\lg x}\right) \leqslant \pi(x) \quad (x \geqslant 599)$$

$$\pi(x) \leqslant \frac{x}{\lg x}\left(1+\frac{1.2762}{\lg x}\right) \quad (x > 1)$$

Dusart 还得到下面不等式：

$$\pi(x) < \frac{x}{\lg x - 1.1} \qquad (x > 60184)$$

$$\pi(x) > \frac{x}{\lg x - 1} \qquad (x > 5393)$$

由 Rosser 和 Schoenfeld(1962) 的结果可知当 $x \geqslant 11$ 时， $\pi(x) \geqslant x/\lg x$.

$\pi(x)$与 $Li(x)$比较

高斯和黎曼相信：对于充分大的 x,$Li(x) > \pi(x)$. 既使这个不等式在目前素数表的范围内是对的，但是 Littlewood 于 1914 年证明了：差数 $Li(x) - \pi(x)$ 有无穷多个地方 $x_0 < x_1 < x_2 < \cdots (x_n \to \infty)$ 变号. 在黎曼猜想之下， Skewes 于 1933 年证明了 $x_0 < 10^{10^{10^{34}}}$. 很长时间以来，这个数是数学中以某种自然方式出现的最大数. 现在既使不假设黎曼猜想， x_0 的上界也已改小了很多.

记录

te Riele 在 1986 年第一个报告了如下计算结果 (发表于 1987 年)：在从 6.62×10^{370} 到 6.69×10^{370} 范围以内，共有 10^{180} 个相邻整数 x, 使得 $Li(x) < \pi(x)$.

4.1E $\zeta(s)$的非平凡零点

回忆：黎曼 zeta 函数有平凡零点 $-2, -4, -6, \cdots$ 和非平凡零点 $\sigma + \mathrm{i}t(0 \leqslant \sigma \leqslant 1)$, 即非平凡零点都在临界带区域中．我先介绍在整个临界带中的零点，然后讨论在临界直线 $\mathrm{Re}(s) = \frac{1}{2}$ 上的零点.

由于 $\zeta(\bar{s}) = \zeta(s)$($\bar{s}$ 表示 s 的共轭复数), 零点关于实轴对称，所以只需考虑临界区域的上半平面部分.

对每个 $t > 0$,zeta 函数只能具有有限多 (如果存在的话) 形如 $\sigma + \mathrm{i}t$ 的零点 (σ 为实数). 所以能够将 zeta 函数的非平凡零点列成 $\rho_n = \sigma_n + \mathrm{i}t_n$, 其中 $0 < t_1 \leqslant t_2 \leqslant t_3 \leqslant \cdots$

对每个 $T > 0$, 以 $N(T)$ 表示 $\zeta(s)$ 在临界带中零点 $\rho_n = \sigma_n + \mathrm{i}t_n$ $(0 < t_n \leqslant T)$ 的个数．类似地， $N_0(T)$ 表示 $\zeta(s)$ 的零点 $\frac{1}{2} + \mathrm{i}t$ $(0 < t \leqslant T)$ 个数．显然 $N_0(T) \leqslant N(T)$, 而黎曼猜想可叙述成：对每个 $T > 0, N_0(T) = N(T)$.

下面是关于 $N(T)$ 的主要结果．首先，下面公式是黎曼的一个猜想，而由 von Mangoldt 证明的

$$N(T) = \frac{T}{2\pi}\left\{\lg\left(\frac{T}{2\pi}\right) - 1\right\} + O(\lg T)$$

由此可知在临界带中有无穷多个零点.

$\zeta(s)$ 目前已知的所有非平凡零点都是单零点． Montgomery 在黎曼猜想之下于 1973 年证明了：至少有三分之二的非平凡零点都是单零点.

1974 年， Levinson 证明了 $\zeta(s)$ 至少有三分之一的非平凡零点在临界直线上．确切地说，对于充分大的 $T, L=\lg(T/2\pi), U=T/L^{10}$, 则

$$N_0(T+U)-N_0(T)>\frac{1}{3}(N(T+U)-N(T))$$

Conrey 在 1989 年又把结果中的 $\frac{1}{3}$ 改进为 $\frac{2}{5}$.

已经算出 $\zeta(s)$ 的许多零点．从 Gram 开始，他在 1903 年算出前 15 个零点 $\rho_n(1\leqslant n\leqslant 15)$. Titchmarsh 在 1935 年算出零点 $\rho_n(n\leqslant 1041)$. 随着计算机的进步， Lehmer 把计算扩大到 $n=35337$.Rosser,Yohe 和 Schoenfeld 在 1969 年计算了前 3500000 个零点.

表 4.2 列出前 30 个零点 $\rho_n=\frac{1}{2}+\mathrm{i}t_n(t_n>0)$.

表 4.2　黎曼 zeta 函数的非平凡零点

n	t_n	n	t_n	n	t_n
1	14.134725	11	52.970321	21	79.337375
2	21.022040	12	56.446248	22	82.910381
3	25.010858	13	59.347044	23	84.735493
4	30.424876	14	60.831779	24	87.425275
5	32.935062	15	65.112544	25	88.809111
6	37.586178	16	67.079811	26	92.491899
7	40.918719	17	69.546402	27	94.651344
8	43.327073	18	72.067158	28	95.870634
9	48.005151	19	75.704691	29	98.831194
10	49.773832	20	77.144840	30	101.317851

在 Edwards 书 (1974) 中详细介绍了 Gram, Backlund, Hutchinson 和 Haselgrove 计算 $\zeta(s)$ 前 300 个零点的方法． Wagon 于 1986 年的短文中对此也作了简要的介绍．从 1977 年 Brent 的工作开始，计算工作扩展得很快．最近发表的结果是 van de Lune,

te Riele 和 Winter(1986) 工作，他们决定了 $\zeta(s)$ 前 1500000001 个非平凡零点都是单零点，都在临界直线上，而虚部 t 满足 $0 < t < 545439823.215$. 这项工作采用一台当时最快的计算机算了 1000 个小时.

记录

S.Wedeniwski 最近宣布他和一个很大的合作队伍计算了 $\zeta(s)$ 的前 10^{11} 个非平凡零点，从而对于 $0 < t < 29538618432.236$ 的情况验证了黎曼猜想.

Odlyzko 和 Schönhage 在 1988 年发明了一种方法，可同时计算 $\zeta(s)$ 的许多零点. 用此法决定了在第 10^{22} 个零点附近的 10^{10} 个零点. Odlyzko(2001) 报告说，这些零点都在临界直线上，这些数据也支持关于 $\zeta(s)$ 的零点与随机矩阵特征值之间联系的另一个猜想的正确性. Odlyzko 认为，如果存在黎曼猜想的反例，它也远在目前已知算法可以达到的范围之外.

人们可能会问：为什么 $\zeta(s)$ 零点在临界直线上这件事是那么重要？这是因为，数学家试图直接证明黎曼猜想的努力至今未能成功，便自然地研究出黎曼猜想的许多推论. 任何一个推论不成立 (并且由黎曼猜想推出这个推论的推导是正确的话) 将意味着黎曼猜想是不对的. 当人们由黎曼猜想推出长期以来所期望得到的许多重要结果的时候，对于要推翻黎曼猜想的对手们更加不利. 当然，这些推论也可能不用黎曼猜想来证明. 但是专家们中的多数人还是坚定地相信黎曼猜想是正确的.

黎曼猜想 (Riemann's hypothesis) 现在被许多人所熟知，我今后将它简记为现已常用的符号 RH. 寻求 RH 推论的工作已经扩大到其他重要的算术领域和几何领域，并且对于比黎曼 zeta 函数更一般的函数 (特别是狄利克雷 L 函数) 引进了各种类型的广义黎

曼猜想 (ERH).

证明 RH 的思路之一可以回溯到希尔伯特，这种思路是在一个适当的希尔伯特空间中寻找一个算子，使它的一批特征值和 zeta 函数的非平凡零点一致，然后由某种对称性推出这些特征值都在临界直线上. 但是如何选择正确的空间，正确的算子和对称性都是非常困难的，最主要的困难是如何把解析的事实融入其中. 作为这方面的记录，建议看 Connes(1996) 的工作.

另一方面，既使目前已经计算出来的 $\zeta(s)$ 的 10^{11} 个非平凡零点都在临界直线上，仍没有给出理性的缘由，说明 RH 是正确的. 也许更大的非平凡零点会发生偏差. 以我们目前的计算能力，对于由一个 lg lg lg 函数所控制的性状或现象仍旧是不能验定的.

4.1F $\zeta(s)$无零点区域和素数定理的误差项

如果知道了 $\zeta(s)$ 有很大的无零点区域，可以对与素数分布有关的各种函数有很好的估计. 我已经提到过， de la Vallée Poussin 决定出一个无零点区域，这是它证明素数定理的最本质因素. 他的结果后来有许多改进. Richert 决定出一个更大的无零点区域，发表于 Walfisz 的书中 (1963)，我这里不打算具体写出这个区域. Kadiri 在 2001 年 (预印本) 发现了 $\zeta(s)$ 如下一个无零点区域:

$$\sigma \geqslant 1 - \frac{1}{5.70233 \times \lg |t|} \quad (|t| \geqslant 3)$$

到目前为止，没有人给出形如 $\{\sigma + \mathrm{i}t | \sigma \geqslant \sigma_0\}$ 的无零点区域，其中 σ_0 是满足 $\frac{1}{2} < \sigma_0 < 1$ 的某个实数.

利用目前已知的 $\zeta(s)$ 无零点区域，可以得到素数定理的误差项估计. 比如说， Tschudakoff(1936) 得到

$$\pi(x) = Li(x) + O(x\mathrm{e}^{-C(\lg x)^{\alpha}})$$

其中 $\alpha < 4/7, C > 0$.von Koch 于 1901 年证明了 RH 等价于

$$\pi(x) = Li(x) + O(x^{1/2} \lg x)$$

知道了 $\zeta(s)$ 的许多零点均在临界直线上，也可得到一些好的估计．例如， Rosser 和 Schoenfeld 在 1975 年证明了

$$0.998684x < \theta(x) < 1.001102x$$

其中下界对 $x \geqslant 1319007$ 成立，而上界对所有 x 均成立．利用 $\zeta(s)$ 的 1.5×10^9 个零点的知识， Dusart 于 1999 年给出一些好的估计．例如，对于 $x > 10544111$

$$|\theta(x) - x| < 0.0066788 \frac{x}{\lg x}$$

对于函数 $\psi(x)$,Rosser 和 Schoenfeld,Dusart 都给出类似的估计．

这些估计常常会打破许多前人的记录，如 Robin(1963),Massias 和 Robin(1996) 的记录．

4.1G　$\pi(x)$的某些性质

在这些方面， Bertrand 通过考查数据历史第一个叙述了下面的猜想 (1845)：

在 $n \geqslant 2$ 和 $2n$ 之间一定有素数．

这等价于说

$$\pi(2n) - \pi(n) \geqslant 1 \qquad (\text{对每个} n \geqslant 1)$$

或者等价于

$$p_{n+1} < 2p_n \qquad (\text{对每个} n \geqslant 1)$$

这通常称之为“Bertrand 猜想”. 它在 1852 年被切比雪夫所证明, 是他对 $\pi(x)$ 所作估计的一个副产品. Bertrand 猜想的一些更简短也可能是最简单的证明后来由 Ramanujan(1919), Erdös(1932) 和 Moser(1949) 发现. 事实上, 更为精细的是下面的不等式:

$$1 < \frac{1}{3}\frac{n}{\lg n} < \pi(2n) - \pi(n) < \frac{7}{5}\frac{n}{\lg n} \qquad (n \geqslant 5)$$

而显然有 $\pi(4) - \pi(2) = \pi(6) - \pi(3) = 1, \pi(8) - \pi(4) = 2$.

更一般地, Erdös 在 1949 年证明了: 对每个 $\lambda > 1$, 均存在 $C = C(\lambda) > 0$ 和 $x_0 = x_0(\lambda) > 1$, 使得

$$\pi(\lambda x) - \pi(x) > C\frac{x}{\lg x} \qquad (x \geqslant x_0)$$

这是素数定理的一个推论.

现在我集中讨论如何用 $\pi(x)$ 和 $\pi(y)$ 来估计 $\pi(xy)$ 和 $\pi(x + y)$.Ishikawa(1934) 的下面结果是切比雪夫定理的一个推论:

$$若 x \geqslant y \geqslant 2, x \geqslant 6, \text{ 则} \pi(xy) > \pi(x) + \pi(y)$$

将 $\pi(x + y)$ 与 $\pi(x), \pi(y)$ 相比较是很有趣的. 基于随机性的考虑, Hardy 和 Littlewood 于 1923 年提出下列猜想 (H-L 猜想):

$$对所有\ x \geqslant 2\ 和\ y \geqslant 2, \pi(x + y) \leqslant \pi(x) + \pi(y).$$

采用更具体的语言, 这个猜想是说: 对每个 $x > 0$ 和任意 y, 在任何区间 $(y, y + x]$(不包含 y, 包含 $x + y$) 中素数的个数不超过区间 $(0, x]$ 中素数的个数, 即 $\pi(y + x) - \pi(y) \leqslant \pi(x)$.

这个猜想看上去是很合理的, 至少它与我们的直观是一致的, 即在整数序列中素数越来越稀疏.

Rosser 和 Schoenfeld 于 1975 年利用他们对 $\theta(x)$ 的估计, 证明了当 $x \geqslant 5$ 时 $\pi(2x) < 2\pi(x)$. Landau 在他的著作 (1913) 中对

充分大的 x 证明了这个不等式. Montgomery 和 Vaughan(1973) 使用更深刻的方法，证明了

$$\pi(x+y) \leqslant \pi(x) + \frac{2y}{\lg y}$$

我在第 4.1E 部分提到过， Rosser 和 Schoenfeld(1975) 还证明了 $y/(\lg y) < \pi(y)$. 所以 $\pi(x+y) \leqslant \pi(x) + 2\pi(y)$.

H-L 猜想则比它更为精致. 在肯定这个猜想方面，除了前面提到的结果外， Udrescu 于 1975 年证明了

对每个 $\varepsilon > 0$ 当 $x, y \geqslant 17$ 和 $x + y \geqslant 1 + \mathrm{e}^{4(1+1/\varepsilon)}$ 时

$$\pi(x+y) < (1+\varepsilon)(\pi(x) + \pi(y))$$

Dusart 于 2002 年研究了满足 H-L 猜想的 (x, y) 组成的集合. 证明了：

若 $2 \leqslant x \leqslant y \leqslant (7/5)x \lg x \lg\lg x$, 则 $\pi(x+y) \leqslant \pi(x) + \pi(y)$

由此可知对每个 $t > \mathrm{e}^{10}$, 均有 $A/t^2 < 5/(7\lg t \lg\lg t)$, 其中 A 是满足 $\pi(x+y) > \pi(x) + \pi(y)$ 的所有 (x, y) 组成的集合的面积 ⑦.

在否定 H-L 猜想方面，我将在 4.4 节讨论 H-L 猜想和 “ k- 素数组猜想” 的关系. 解释这两个猜想是相互排斥的.

下面两个命题至今也都未被证明或者推翻：

Opperman 于 1882 年推断：对每个 $n > 1, \pi(n^2+n) > \pi(n^2) > \pi(n^2-n)$.

Brocard 于 1904 年论断：对每个 $n \geqslant 2, \pi(p_{n+1}^2) - \pi(p_n^2) \geqslant 4$. 换句话说，任意两个大于 2 相邻素数的平方之间至少有 4 个素数.

---

⑦ 应再加条件 $0 \leqslant x, y \leqslant t$—— 译者注.

4.1H 欧拉函数值的分布

这里我收集欧拉函数值的一些分布结果. 它们是第二章 2.2 节所叙述的一些性质的补充.

首先介绍欧拉函数的增长性状. 不难证明

$$\varphi(n) \geqslant \lg 2 \frac{n}{\lg(2n)}$$

特别对每个 $\delta > 0$, $\varphi(n)$ 的增长比 $n^{1-\delta}$ 要快. 还可做得更好: 对每个 $\varepsilon > 0$ 均存在 $n_0 = n_0(\varepsilon)$, 使得当 $n \geqslant n_0$ 时

$$\varphi(n) \geqslant (1-\varepsilon)\mathrm{e}^{-\gamma} \frac{n}{\lg \lg n}$$

另一方面, 由素数定理可以推出, 存在无穷多个 n, 使得

$$\varphi(n) \leqslant (1+\varepsilon)\mathrm{e}^{-\gamma} \frac{n}{\lg \lg n}$$

因此

$$\liminf \frac{\varphi(n) \lg \lg n}{n} = \mathrm{e}^{-\gamma}$$

这些结果的证明可见 Landau(1909) 和 Apostol(1976) 的书.

$\varphi(n)$ 的平均值如何? 由关系式 $n = \sum\limits_{d|n} \varphi(d)$ 不难证明

$$\frac{1}{x} \sum_{n \leqslant x} \varphi(n) = \frac{3x}{\pi^2} + O(\lg x)$$

所以 $\varphi(n)$ 的平均值为 $3n/\pi^2$. 由此可以推出: 如果随机地取两个整数 $n, m \geqslant 1$, 它们互素的概率为 $6/\pi^2$.

所有这些事情在 Hardy 和 Wright 的书以及 Apostol 的书 (1976) 中均有很好的论述.

4.2 第 n 个素数和素数的间隙

上节中我们介绍了函数 $\pi(x)$, 它的渐近性状、与已知函数的比较以及一些其他性质. 但是没有谈 $\pi(x)$ 在小区间中的性状, 第 n 个素数的大小和相邻素数之差等. 这些问题属于素数分布的更精细考虑, 而且预料在这些方面更加不规则.

4.2A 第 n个素数

现在比较专门地考虑第 n 个素数 p_n. 由素数定理不难得到

$$p_n \sim n \lg n, \qquad 即 \lim_{n\to\infty} \frac{p_n}{n \lg n} = 1$$

换句话说, 对充分大的 n, 第 n 个素数的大小约为 $n \lg n$. 更精确地有

$$p_n = n \lg n + n(\lg \lg n - 1) + O\Big(\frac{n \lg \lg n}{\lg n}\Big)$$

所以对于充分大的 n, $p_n > n \lg n$. 但是 Rosser 于 1938 年证明了:

对每个 $n > 1$

$$n \lg n + n(\lg \lg n - 10) < p_n < n \lg n + n(\lg \lg n + 8)$$

并且对每个 $n \geqslant 1, p_n > n \lg n$.Dusart 于 1999 年证明了: 对于 $n > 39017, p_n < n(\lg n + \lg \lg n - 0.9484)$, 并且对每个 $n > 1, p_n > n(\lg n - \lg \lg n - 1)$.

下列结果由 Ishikawa(1934) 证明, 它是切比雪夫定理的一个推论 (见一般参考文献中 Trost 的书):

若 $n \geqslant 2$, 则 $p_n + p_{n+1} > p_{n+2}$; 若 $m, n \geqslant 1$, 则 $p_m p_n > p_{m+n}$.

Dusart 于 1998 年还证明了 R.Mandl 下面的猜想 (见 Rosser

和 Schoenfeld　1975) 是对的

$$\text{当}n \geqslant 9\text{时}, \quad \frac{p_1 + p_2 + \cdots + p_n}{n} \leqslant \frac{1}{2}p_n$$

Pomerance 在 1979 年一篇有趣的文章中考虑素数图，这个图的顶点是平面上全部点 (n, p_n) $(n \geqslant 1)$. 他证明了 Selfridge 的一个猜想：存在无穷多个 n, 使得对每个小于 n 的正整数 i, 均有 $p_{n^2} > p_{n-i}p_{n+i}$. 并且有无穷多个 n, 使得对每个小于 n 的正整数 i, 均有 $2p_n < p_{n-i} + p_{n+i}$.

F.Firoozbakht 在 1992 年写信给我，说他有一个新的猜想. 据我所知这个猜想还未发表过. 这个猜想是说：序列 $\left(p_n^{1/n}\right)_{n \geqslant 2}$ 是严格递降的. 从而在关于素数的似乎无穷多个合理的推断中又增加了一个. 这些推断在很大范围都得到数值的验证 (否则的话，它们就被扔到“数学垃圾堆”里去了). 但是面对这么多的情形，我们这些聪明的数学家们不能决定哪些推断是正确的或者是错误的.

4.2B　素数间隙

素数定理告诉我们当 x 趋于无穷时函数 $\pi(x)$ 是如何增长的. 为了更详细地理解素数的分布，需要研究相邻素数差 $d_n = p_{n+1} - p_n$.

一个素数 p 的间隙 $g(p)$ 定义为在它后面连续有多少个合成数，即 $p_{n+1} = p_n + g(p_n) + 1$. 注意当 $p > 2$ 时， $g(p)$ 为奇数. 称 $g(p_n)$ 是一个最大间隙，是指对所有 $p_k < p_n$ 均有 $g(p_n) > g(p_k)$.

考虑 $g(p)$ 的所有可能取值组成的集合 $G = \{m |$ 存在某个$p > 2$, 使得 $m = g(p)\}$. 对每个 $m \in G$, 以 $p[m]$ 表示满足 $g(p) = m$ 的最小素数 p. 在文献中 $p[m]$ 叫作间隙 m 的第一次出现.

在间隙 (即相邻素数差) 的研究中讨论了以下一些问题：当 n 趋于无穷时 d_n 的性状；集合 G 的性质；间隙的第一次出现； d_n

的增长速度；以及迭代间隙.

当 n 趋于无穷时 d_n 的性状

容易证明 $\limsup d_n = \infty$. 这意味着对每个 $N > 1$, 均存在连续 N 个合成数. 例如

$$(N+1)!+2, (N+1)!+3, (N+1)!+4, \cdots, (N+1)!+(N+1)$$

实际上，实验中发现的连续 N 个合成数比 $(N+1)!$ 要小得多. 所以更引人注意的问题是对比较小的 n 决定大的间隙 d_n. 我们在后面将要定义一个"间隙度"概念.

与 $\limsup d_n$ 相比， $\liminf d_n$ 至今没有解决 (当然 $\liminf d_n$ 是存在的). 下面考查想像中的各种可能性:

- $\liminf d_n = \infty$. 这意味着对每个 k 均只有有限多个素数 p_n, 使得 $d_n = 2k$. 这也相当于说：对每个 k 均存在 n_0, 使得当 $n > n_0$ 时，均有 $p_n > 2k$. 这件事对吗？
- 存在某个 $l \geqslant 1$, 使得 $\liminf d_n = l$. 这意味着有无限多个素数 p_n 使得 $d_n = l$, 并且 l 是具有此性质的最小整数. 对任何 l 我们都不知道这个命题是否成立.

这些问题与下面的猜想有密切联系.

Polignac 猜想 (1849) *对每个偶数 $2k(k \geqslant 1)$, 均存在无穷多对相邻素数 p_n 和 p_{n+1}, 使得 $d_n = p_{n+1} - p_n = 2k$.*

特别地 $k = 1$,Polignac 猜想是说有无穷多个素数 p, 使得 $p+2$ 也是素数. 这就是著名的孪生素数猜想. 将在 4.3 节中研究.

我还要强调，既使连下面的猜想也还没有解决：对每个 $k > 1$ 均存在一对素数 p 和 q(不必相邻), 使得 $q - p = 2k$.

集合 G(素数可能的间隙)

Powell 在《美国数学月刊》(*American Mathematical Monthly*) (1983) 中提了如下的问题:

对每个自然数 M 均存在一个偶数 $2k$, 使得至少有 M 个相邻素数对的差为 $2k$.

这个问题由 Davies 于 1984 年证明, 是素数定理一个简单的应用.

证明 对于充分大的 n, 考虑素数序列

$$3 = p_2 < p_3 < \cdots < p_n$$

和 $n-2$ 个素数差 $p_{i+1} - p_i (2 \leqslant i \leqslant n-1)$. 如果不同差值的个数小于 $\left[\dfrac{n-2}{M}\right]$, 则其中某个差数 (记为 $2k$) 将出现多于 M 次. 因为不然的话

$$p_n - p_2 \geqslant 2 + 4 + \cdots + 2\left[\frac{n-2}{M}\right]$$

但是右边渐近地等于 n^2/M^2, 而左边渐近地等于 $n \lg n$(素数定理), 这是不可能的. □

上面的结果还可表达成: 对每个自然数 M 都存在奇数 $m \in$ G, 使得 $g(p) = m$ 的素数 p 多于 M 个.

目前不知道是否每个正偶数都为相邻素数之差, 这在前面研究与 Polignac 猜想的关系时曾经提到过. 所以我们也不知道 G 是否包含所有的正奇数.

对于某个范围以内的数, 已经决定了它是否为 (某些“小”) 素数的间隙, 也发现了相邻素数之间一些特别大的间隙. Dubner 给出一个算法, 用这个算法对每个奇数 $m < 10180$, 均决定出一个素数 p, 使得 p 后面恰好有连续 m 个合成数. 在这个范围内给出的 $p[m]$ 的上界高达 398 位.

记录

J.L.Gómez Pardo 于 2002 年 3 月明确地决定了最大相邻素数间隙：在一个 3474 位的素数后面恰好有 112193 个合成数．这些数的素性判定分别由 M.Ladra 和 M.Seijas 做出，利用了 M.Martin 性能良好的 ECPP 软件．

第一次出现和间隙度

已经制作了不少 $p[m]$ 的数据表．由这些表可从中找出具有给定最大间隙的素数．这些表按发表的顺序为：Lander 和 Parkin(1967), Brent (1973, 1980),Young 和 Potler(1989) 和 Nicely(1999)．这些计算又被 Nicely, B.Nyman 和 T.Oliveira e Silva 所扩大，他们一起审查了 $N = 6 \times 10^{16}$ 以内的全部素数．

记录

最大间隙的最大值是由 Oliveira e Silva 在 2002 年 9 月发现的，它为 $m = 1197$, 而 $p[m] = 55350776431903243$. 在此之前的记录是 Nyman 的： $m = 1183$(2002 年) 和 $m = 1131$ (1999 年)．更早时候为 $m = 803$[Young 和 Potler(1989)] 和 $m = 651$[Brent(1973)].

当然，若 m 不是上述表格范围之内的 $g(p)$ 值，则需要进一步做专门的研究．有许多年人们不能确定间隙 $m = 999$ 何时第一次出现，但是 Nyman 最近 (2001 年 5 月) 发现 $p[999] = 22439962446379651$. 目前，第一次出现不能确定的最小的间隙为 $m = 1047$.Oliveira e Silva 给出一个上界 $p[1047] \leqslant 88089672331629091$.

关于 $p[m]$ 的渐近性状， Shanks 于 1964 年猜想当 m 趋于无穷时， $\lg p[m] \sim \sqrt{m}$.Weintraub 根据他自己的大量计算，于 1991

年建议为

$$\lg p[m] \sim \sqrt{1.165746m}$$

如果对某个素数 p 知道间隙 $g(p)$(不必是第一次出现), 自然要问：它在这样大小的素数当中是否为“特别大”的间隙？由素数定理可知，在 p 附近的素数之间平均间隙近似于 $\lg p$. 所以可以定义间隙度 $g(p)/\lg p$：一个间隙“特别大”即指间隙度很大.

目前所知具有最大间隙度的素数为 Nyman 发现的 $p = 1693182318746371$, 其中 $g(p) = 1131$(这也是一个最大间隙), 间隙度为 32.25. 次好的间隙度为 31.05, 是上面所述 Oliveira e Silva 创记录的最大间隙 1197. 相比之下，对于目前计算出来的最大的间隙 112193, 其间隙度为 14.03.

d_n的增长速度

这项研究的指导思想很简单：寻求一个可与 d_n 相比较的尽量简单和容易计算的正实值函数 $f(p_n)$. 通常 $f(p_n)$ 包含方幂和对数，而相比较是指如下一类问题：

$$d_n = O(f(p_n))? \quad d_n = o(f(p_n))? \quad d_n \sim f(p_n)?$$

让我们从切比雪夫关于 Bertrand 猜想的古老结果开始，这个结果是说：对每个 $n \geqslant 1$, 均有 $d_n < p_n$. 由素数定理可知

$$\lim_{n\to\infty} \frac{d_n}{p_n} = 0$$

由于对每个 $n \geqslant 1$ 均有 $d_n < p_n$, 可知 $d_n = O(p_n)$. 一个自然的问题是求满足 $d_n = O(f(p_n))$ 的最好的函数 $f(p_n)$.

数学家们希望在不用黎曼猜想之下，能证明对每个 $\varepsilon > 0$ 均有 $d_n = O(p_n^{1/2+\varepsilon})$. 通过一系列的竞赛，现在离这个界已经很近了. 第一个结果是 Hoheisel(1930) 的 $d_n = O(p_n^{\theta})$, 其中 θ

只比 1 小一点. 然后经过 Ingham(1937),Montgomery (1969),Huxley(1972),Iwaniec 和 Jutila(1979),Heath-Brown 和 Iwaniec(1979) 和 Iwaniec 和 Pintz(1984) 的结果, 一直到最近的记录.

记录

目前记录为 Baker,Harman 和 Pintz(2001) 的 $\theta = 0.525$. Mozzochi (1986) 曾给出 $\theta = 1051/1920 \approx 0.5474$, 而 Lou 和 Yao 在 1993 年得到稍好一点的 $\theta = 6/11 \approx 0.5454$.

以上结果涉及 d_n 的增长 (当 n 趋于无穷时). 另一方面, Ramaré 和 Saouter(2003) 通过计算, 对于包含素数的短区间积累了丰富的知识: 令 $x_0 = 10\ 726\ 905\ 041$ 和 $\Delta = 28\ 314\ 000$. 如果 $p_n > x_0$, 则 $d_n < p_{n-1}/\Delta$.

由素数定理可推得 d_n 的数量级为 $\lg p_n$, 即 $d_n/\lg p_n \sim 1$. 但是间隙值与期望值仍有偏差. 在黎曼猜想下, Cramér 于 1937 年证明了 $d_n = O(p_n^{1/2} \lg p_n)$. 基于概率的推断, Cramér 猜想 $d_n = O((\lg p_n)^2)$.

对于小于期望值的情形有以下一些结果. 首先, Erdös 于 1940 年证明了: 存在常数 $C(0 < C < 1)$, 使得

$$\liminf \frac{d_n}{\lg p_n} < C$$

然后有许多人估计 C.Bombieri 和 Davenport 于 1966 年证明 C 可取为 0.467, 这个后来被 Huxley(1977) 稍加改进, 目前最好结果为 Maier(1985) 的 0.248.

关于大间隙方面, Westzynthius 于 1931 年证明了 $\limsup d_n/\lg p_n = \infty$, 这意味着对每个 $t > 0$, 均有无穷多个 $n > 0$, 使得 $p_{n+1} > p_n + t \lg p_n$.

从 1938 年起, Rankin 继续 Erdös(1935) 的工作, 到 1963 年

改进为：存在无穷多 n, 使得

$$\frac{d_n}{\lg p_n} \geqslant l_n \mathrm{e}^{\gamma} = l_n \times 1.78107\cdots.$$

其中 γ 为欧拉常数，而

$$l_n = \frac{(\lg_2 p_n)(\lg_4 p_n)}{(\lg_3 p_n)^2} > 1$$

Erdös 设 10000 美元奖，奖给能把 Erdös-Rankin 不等式中 e^{γ} 改成 ∞ 的人.

下面是另一个未解决的问题：证明

$$\lim_{n\to\infty}(\sqrt{p_{n+1}} - \sqrt{p_n}) = 0$$

如果这个成立, 则 D.Andrica 猜想 $\sqrt{p_{n+1}} - \sqrt{p_n} < 1$ 对于充分大的 n 成立. 反之若此不等式成立, 则在任何两个相邻整数的平方之间必有素数. 后者似乎是对的，但也未被证明. 注意这比 Opperman 猜想要弱.

Andrica 猜想的正确性目前已验证到 $n \leqslant 2^{42} \approx 4.39 \times 10^{12}$. 还要注意：这个不等式等价于 $g(p_n) < 2\sqrt{p_n}$(其中 $g(p_n)$ 为间隙 $p_{n+1} - p_n$). 而后一不等式只对 N 之内的最大间隙验证即可，由此即可推出 Andrica 不等式对所有 $p_n < N$ 成立. 用 Nicely 关于第一次出现间隙的表格，目前这已作到 $N = 6 \times 10^{16}$.

迭代间隙

1878 年 Proth 研究素数之间的迭代间隙. 令 $p_1 = 2, p_2 = 3, \cdots, p_n, p_{n+1}, \cdots$ 为素数序列. 对 $n \geqslant 1$ 令 $\delta_1(n) = |p_{n+1} - p_n| = d_n$. 更一般地，对 $k \geqslant 1$, 令 $\delta_{k+1}(n) = |\delta_k(n+1) - \delta_k(n)|$. 由此给

出如下序列：

2	3	5	7	11	13	17	19	23	29	⋯
1	2	2	4	2	4	2	4	6		
1	0	2	2	2	2	2	2			
1	2	0	0	0	0	0				
1	2	0	0	0	0					
1	2	0	0	0						
1	2	0	0							
1	2	0								等等

对每个 $k(1 \leqslant k \leqslant 7)$，均有 $\delta_k(1) = 1$. Proth 声称他证明了对所有 $k \geqslant 1$ 均成立，但他的证明是错的. N.L.Gilbreath 在不知道 Proth 工作的情况下于 1950 年前后 (未发表) 又叙述了同样的猜想. Killgrove 和 Ralston 在 1959 年验证了此猜想对 $k \leqslant 63\,419$ 是对的. 1993 年 Odlyzko 对于所有 $k \leqslant 3.46 \times 10^{11}$(即一直到 10^{13} 的素数) 验证了 $\delta_k(1) = 1$.

间隙和联姻问题

联姻问题和素数间隙有什么关系？在附录 1 “联姻和素数”中会找到答案. 这个附录是 M.Ram Murty 送给我的礼物. 他是这个题目中半个题目的专家，而我在过去的 50 年从事了另半个题目的实践. 这是一个值得仿效的例子，就像在其他艺术领域那样，一首诗是献给某个朋友的礼物.

4.3 孪生素数

若 p 和 $p+2$ 均为素数，它们叫作孪生素数.

前四个孪生素数对为 $(3,5),(5,7),(11,13),(17,19)$.Clement 于

1949 年对孪生素数做了如下刻画:

设 $n \geqslant 2$, n 和 $n+2$ 是孪生素数对当且仅当

$$4[(n-1)!+1]+n \equiv 0 \pmod{n(n+2)}$$

证明 若同余式成立, 则 $n \neq 2,4$, 并且 $(n-1)!+1 \equiv 0 \pmod{n}$. 由 Wilson 定理知 n 为素数. 同时有

$$4(n-1)!+2 \equiv 0 \pmod{n+2}$$

乘以 $n(n+1)$ 之后

$$4[(n-1)!+1]+2n^2+2n-4 \equiv 0 \pmod{n+2}$$

于是

$$4[(n+1)!+1]+(n+2)(2n-2) \equiv 0 \pmod{n+2}$$

再由 Wilson 定理知 $n+2$ 也是素数.

反之, 若 n 和 $n+2$ 都是素数, 则 $n \neq 2$ 并且

$$(n-1)!+1 \equiv 0 \pmod{n}$$
$$(n+1)!+1 \equiv 0 \pmod{n+2}$$

但是 $n(n+1)=(n+2)(n-1)+2$, 所以 $2(n-1)!+1=k(n+2)$, 其中 k 为整数. 由 $(n-1)! \equiv -1 \pmod{n}$, 可知 $2k+1 \equiv 0 \pmod{n}$. 代入前式得到 $4(n-1)!+2 \equiv -(n+2) \pmod{n(n+2)}$, 所以 $4[(n-1)!+1]+n \equiv 0 \pmod{n(n+2)}$. □

这个刻画方法对于决定孪生素数没有实际价值.

孪生素数主要问题是：是否存在无穷多孪生素数对． 1919 年， Brun 证明了一个著名的结果，即和式

$$\left(\frac{1}{3}+\frac{1}{5}\right)+\left(\frac{1}{5}+\frac{1}{7}\right)+\left(\frac{1}{11}+\frac{1}{13}\right)+\cdots+\left(\frac{1}{p}+\frac{1}{p+2}\right)+\cdots$$

收敛于一个数 B, 其中求和过所有孪生素数对 $(p, p+2)$.B 现在叫 Brun 常数.

这个结果并不排除存在无穷多对孪生素数的可能性，但告诉我们这些孪生素数对会越来越远，从而使它们的倒数之和为有限的实数.

基于孪生素数分布的数据经验， Shanks 和 Wrench(1974), Brent (1976) 等都对 B 作了计算，较近的结果是 Nicely(2001) 得到

$$\mathrm{B}=1.9021605823\cdots$$

Brun 还证明了：对每个 $m \geqslant 1$ 均存在连续 m 个素数都不是孪生素数.

对每个 $x>1$, 以 $\pi_2(x)$ 表示满足 $p+2 \leqslant x$ 的孪生素数对 $(p, p+2)$ 的个数. Brun 在 1919 年宣称：存在一个有效可计算的整数 x_0, 使得当 $x \geqslant x_0$ 时,

$$\pi_2(x)<\frac{100 x}{(\lg x)^2}$$

证明出现于 1920 年.

$\pi_2(x)$ 的上界归结于决定常数和误差项大小. Bombieri 和 Davenport 于 1966 年作了此事. 证明可见 Halberstam 和 Richert 的书，它是筛法的一个应用. 结果为

$$\pi_2(x) \leqslant 2 C \prod_{p>2}\left(1-\frac{1}{(p-1)^2}\right) \frac{x}{(\lg x)^2}$$

关于 C 的最好值为 Bombieri, Friedlander 和 Iwaniec(1986) 的 C=3.5 和 S. Lou(楼世拓，私人通信) 的 $C = 3.13$. 更早些时候，Hardy 和 Littlewood(1923) 根据经验，猜想有

$$\pi_2(x) \sim C_2 \frac{x}{(\log_2 x)^2}$$

其中无穷乘积

$$C_2 = \prod_{p>2} \left(1 - \frac{1}{(p-1)^2}\right)$$

叫作孪生素数常数 (见第六章 6.4 节).Wrench 于 1961 年计算出 $C_2 = 0.66016\cdots$ 为了弄清楚常数 C_2,Hardy 和 Littlewood 的经验式的理由后来由其他作者加以解释，并且由 Golomb (1960) 进一步加以简化. 我想有必要描述一下给出常数 C_2 的理由，尽管推理并不是很严格的.

由素数定理可知 $\pi(x)/x \sim 1/\lg x$, 所以正整数 n 为素数的概率是 $1/\lg n$. 而 $n+2$ 为素数的概率也是一样的. 所以若这两个事件是独立的，则 n 和 $n+2$ 同时为素数的概率为 $1/(\lg n)^2$. 但是这两个事件不是独立的. 因为若 $n > 2$ 为素数，则 n 为奇数，所以 $n+2$ 也是奇数. 考虑到 $n+2$ 在奇数子集合中，它为素数的概率应当加一个矫正因子 2.

对每个奇素数 $p \neq n$,n 属于 $(p-1)/p$ 个同余类当中的一个. 如果 $n+2$ 也是素数，并且 $p \nmid n+2$, 则 $n+2$ 属于前面 $(p-2)/(p-1)$ 个同余类当中的一个. 所以对每个素数 $p > 2$, 在计算概率时要考虑加上因子

$$\frac{p-2}{p-1} \bigg/ \frac{p-1}{p} = \frac{p(p-2)}{(p-1)^2} = 1 - \frac{1}{(p-1)^2}$$

从而根据这种经验考虑， $\pi_2(n)/n$ 应为 $C_2/(\lg n)^2$.

为了对 $\pi_2(x)$ 的增长状况有所感觉，我取出 Brent(1975, 1976) 和 Nicely(1995, 2001) 的一部分计算结果列成表 4.3.

表 4.3　孪生素数对的个数

x	$\pi_2(x)$
10^3	35
10^4	205
10^5	1 224
10^6	8 169
10^7	58 980
10^8	440 312
10^9	3 424 506
10^{10}	27 412 679
10^{11}	224 376 048
10^{12}	1 870 585 220
10^{13}	15 834 664 872
10^{14}	135 780 321 665
10^{15}	1 177 209 242 304

记录

关于不超过一给定数 x 的孪生素数对的个数 $\pi_2(x)$, 其最大的确切值是由 Nicely 于 2003 年 2 月算出的

$$\pi_2(4.35 \times 10^{15}) = 4698614557533$$

记录

表 4.4 给出已知的最大孪生素数对.

如果 $2k$ 个相邻素数形成 k 个孪生素数对，称之为 k 阶孪生素数束. 是否存在任意阶的孪生素数束，是一个未解决的问题. 但是它可以由 Dickson 的另一个未被证明的猜想 (见第六章 6.1 节的 D_3) 推出来. N.B.Backhouse 告诉我 1~7 阶的最小孪生素数束，它们的起始素数分别为 $3, 5, 5, 9419, 909287, 325267931, 678771479$.

表 4.4　已知的最大孪生素数对

素数对	位数	发现者	时间 (年)
$33218925 \times 2^{169690} \pm 1$	51090	D.Papp, P.Jobling, G.Woltman and Y.Gallot	2002
$60194061 \times 2^{114689} \pm 1$	34533	D.Underbackke, G.Woltman and Y.Gallot	2002
$1765199373 \times 2^{107520} \pm 1$	32376	J.McElhatton and Y.Gallot	2002
$318032361 \times 2^{107001} \pm 1$	32220	D.Underbakke, P.Carmody, C.Nash et al.	2001
$1807318575 \times 2^{98305} \pm 1$	29603	D.Underbakke, P.Carmody, and Y.Gallot	2001
$665551035 \times 2^{80025} \pm 1$	24099	D.Underbakke, P.Carmody and Y.Gallot	2000
$781134345 \times 2^{66445} \pm 1$	20011	D.Underbakke, P.Carmody, C.Nash et al.	2001
$1693965 \times 2^{66443} \pm 1$	20008	G.La Barbera, P.Jobling and Y.Gallot	2000
$83475759 \times 2^{64955} \pm 1$	19562	D.Underbakke, P.Jobling and Y.Gallot	2000
$291889803 \times 2^{60090} \pm 1$	18098	D.Boivin and Y.Gallot	2001

记录

最小的 8 阶孪生素数束是由 P.Carmody 于 2001 年 1 月发现的，它的起始素数为 1107819732821. 最小的 9 阶孪生素数束是由 D. DeVries 和 P. Sebah 于 2002 年 3 月发现的，起始素数为 170669145704411.

已经有许多人试图用筛法来证明存在无穷多对孪生素数. Brun 在 1920 年的著名文章中证明了 2 可以有无穷多种方法表示成 $2 = m - n$, 其中 m 和 n 都最多 9 个 (不必不同的) 素数之乘积.

目前最好的结果是陈景润于 1966 年得到的 (发表于 1973, 1978). 他证明了 2 可以有无穷多种方法表示成 $2 = m - p$, 其中 p 为素数，而 m 是至多两个 (不必不同的) 素数之乘积.

用于研究孪生素数的筛法也可研究哥德巴赫问题 (见 4.6 节).

4.2 节的一般 Polignac 猜想也可部分地按孪生素数猜想的方式研究. 对于 $k \geqslant 1$ 和 $x > 1$, 以 $\pi_{2k}(x)$ 表示满足 $p_{n+1} \leqslant x$, $p_{n+1} - p_n = 2k$ 的整数 $n > 1$ 的个数. 采用 Brun 筛法, 可以证明存在一个常数 $\mathrm{C}_k > 0$, 使得

$$\pi_{2k}(x) < \mathrm{C}_k \frac{x}{(\lg x)^2}$$

4.4 k- 素数组

前面我考虑了孪生素数对 $(p, p+2)$. 这是具有最小可能差值 2 的两个相邻素数. 类似地, 可以定义 3- 素数组 (p_0, p_1, p_2), 其中 $p_0 < p_1 < p_2$ 并且具有最小可能的差值 $p_2 - p_1$. 这样的 3- 素数组共有两类: $(p, p+2, p+6)$(如 $(11, 13, 17)$) 和 $(p, p+4, p+6)$(如 $(7, 11, 13)$). 另一方面, 若 $p, p+2, p+4$ 均为素数, 则只有 $p = 3$, 因为这三个数当中必有一个被 3 整除.

4- 素数组 (p_0, p_1, p_2, p_3) 是指 $p_0 < p_1 < p_2 < p_3$ 为相邻素数, 并且 $p_3 - p_0$ 达到最小可能. 由于 $p, p+2, p+4, p+6$ 不能同时为素数, 所以最小差值不能为 6. 但是 $11, 13, 17, 19$ 均为素数, 所以最小差值为 8, 并且 $(11, 13, 17, 19)$ 是 4- 素数组. 而每个 4- 素数组必为形式 $(p, p+2, p+6, p+8)$.

更一般地, 对于 $k \geqslant 2$, 假设

(i) $b_1 < b_2 < \cdots < b_{k-1}$;

(ii) $p, p+b_1, \cdots, p+b_{k-1}$ 是 k 个相邻素数;

(iii) 不存在素数序列 $q_0 < q_1 < \cdots < q_{k-1}$ 使得 $q_{k-1} - q_0 < b_{k-1}$.

则 $(p, p+b_1, \cdots, p+b_{k-1})$ 叫作是一个 k- 素数组,而 $(b_1, b_2, \cdots, b_{k-1})$ 叫作 k- 素数组的类型.

现在我引入下列记号:对每个实数 $x>0$, 令

$$\pi_{2,6}(x)=\#\{3\text{- 素数组}(p,p+2,p+6)|\ p\leqslant x\}$$

$$\pi_{4,6}(x)=\#\{3\text{- 素数组}(p,p+4,p+6)|\ p\leqslant x\}$$

类似地

$$\pi_{2,6,8}(x)=\#\{4\text{- 素数组}(p,p+2,p+6,p+8)|\ p\leqslant x\}$$

又令

$$B_{2,6} = \sum\left(\frac{1}{p}+\frac{1}{p+2}+\frac{1}{p+6}\right)$$

$$B_{4,6} = \sum\left(\frac{1}{p}+\frac{1}{p+4}+\frac{1}{p+6}\right)$$

$$B_{2,6,8} = \sum\left(\frac{1}{p}+\frac{1}{p+2}+\frac{1}{p+6}+\frac{1}{p+8}\right)$$

其中求和分别过相应的 3- 素数组和 4- 素数组. 就像孪生素数对 $(p,p+2)$ 关于倒数和的 Brun 结果那样,上面诸和式也都是收敛的. 当然这与相应 k- 素数组的无穷性质并不矛盾.

T.R.Nicely 1999 年告诉我:对于 $N=1.5\times10^{15}$

$$\pi_{2,6}(N)=110261940034$$

$$\pi_{4,6}(N)=110262203391$$

$$\pi_{2,6,8}(N)=4737286827$$

记录

下面对 $k \geqslant 3$ 给出已知的最大 k- 素数组的明显例子，来源于 T.Forbes.

(1) 3- 素数组 $(p, p+2, p+6)$, $p=(90159302514 \times d(d+1)+210)(d-1)/35+5$, 其中 $d=4436 \times 3251\#$ (4135 位， D.Broadhurst 等 2002)

(2) 3- 素数组 $(p, p+4, p+6)$, $p=(108748629354 \times d(d+1)+210)(d-1)/35+7$, 其中 $d=4436 \times 3251\#$ (4135 位， D.Broadhurst 等 2002)

(3) 4- 素数组 $(p, p+2, p+6, p+8)$, $p=10271674954 \times 2999\#+3461$ (1284 位， M.Bell 等 2002)

(4) 5- 素数组 $(p, p+2, p+6, p+8, p+12)$, $p=31969211688 \times 2399\#+16061$ (1034 位， N.Luhn 等 2002)

作为实际计算的成就，最大的 17- 素数组为

$$
\begin{aligned}
&(p, p+6, p+8, p+12, p+18, p+20, p+26, p+32, p+36, \\
&\quad p+38, p+42, p+48, p+50, p+56, p+60, p+62, p+66), \\
&\quad p=2845372542509911868266811
\end{aligned}
$$

(25位， J.Waldvogel 和 P.Leikauf 2000)

当 k 较小时，已有很多 k- 素数组的例子. 但是 k 很大时情况完全不同，找到一个 k- 素数组都很困难. 当 $k=10^{10^{10}}$ 时我们能做些什么？怎样才能知道至少存在一个 k- 素数组？这是很有趣的问题，现在较详细地作一介绍.

设 $k \geqslant 2$. 一个 $(k-1)$- 整数组 $(b_1, b_2, \cdots, b_{k-1})$ 叫作是允许的，是指

(i) $b_1<b_2<\cdots<b_{k-1}$;

(ii) 对每个素数 $q<k$. 同余类集合 $\{0, b_1, b_2, \cdots, b_{k-1} \pmod{q}\}$

为模 q 所有同余类的真子集.

如果 $(b_1,b_2,\cdots,b_{k-1})$ 是允许的，取 $q=2$ 可知 b_i 均为偶数. 在所有允许 $(k-1)$- 整数组当中取 b_{k-1} 最小者的那些叫作严紧的 (tight). 例如，对 $k\leqslant 4$, 严紧的 $(k-1)$- 允许整数组为 (2),(2,6),(4,6), (2,6,8).

我们采用 Hensley 和 Richards(1974) 中的记号， $\rho^*(x)=k$ 表示存在允许的 $(k-1)$- 数组 $(b_1,b_2,\cdots,b_{k-1})$ 使得 $b_{k-1}<x$, 但是不存在多于 $k-1$ 个分量的这种数组. 对每个 x 都可通过有限步算出 $\rho^*(x)$ 来. 但是当 x 很大时，这是一个复杂的组合问题.

在 Hardy 和 Littlewood(1923),Schinzel 和 Sierpiński(1958) 和其他作者的工作中也曾考虑过类似的函数. 特别是考虑过

$$\rho(x)=\limsup_{y\to\infty}\left(\pi(x+y)-\pi(y)\right)$$

我们有 $\rho(x)\leqslant\rho^*(x)$.

证明 设 $\rho(x)=k$, 则存在 $y\geqslant k$ 和 k 个素数 $p+b_i$ $(0\leqslant i\leqslant k-1,\ b_0=0)$, 使得 $y<p<p+b_1<\cdots<p+b_{k-1}\leqslant y+x$. 于是 $b_{k-1}<x$. 如果存在素数 $q\leqslant k$, 使得 $\{b_i \mod q\mid 0\leqslant i\leqslant k-1\}$ 为模 q 全部同余类, 则有 i 使得 $-p\equiv b_i\ (\mathrm{mod} q)$, 于是 $q\mid p+b_i$, 从而 $q\leqslant k\leqslant y\leqslant p+b_i=q$, 而这是不可能的. 所以 $(b_0,b_1,\cdots,b_{k-1})$ 是允许的，这表明 $k\leqslant\rho^*(x)$. □

一个很有趣的问题是比较 $\pi(x)$ 和 $\rho^*(x)$. 数值计算始于 Schinzel (1961), 而 Selfridge (未发表) 对 $x\leqslant 500$ 证明了 $\rho^*(x)\leqslant\pi(x)$. 但是 Hensley 和 Richards(1974) 的以下定理表明这种情况是极为罕见的：

对每个 $\varepsilon,0<\varepsilon<\lg 2$, 均存在 $x_0>1$, 使得当 $x\geqslant x_0$ 时

$$\rho^*(x) - \pi(x) > (\lg 2 - \varepsilon)\frac{x}{(\lg x)^2}$$

特别地， $\lim_{x\to\infty}(\rho^*(x) - \pi(x)) = \infty$

利用一个精心设计的计算机程序， W.Stenberg 在 1974 年得到 $\rho^*(20000) > \pi(20000)$. 一个困难问题是决定 $\rho^*(x)$ 的阶. 是否 $\rho^*(x) \sim \pi(x)$ ？

下面猜想特别可以推出 k- 素数组的存在性.

k- 素数组猜想 设 $k \geqslant 2$, 而 $(b_1, b_2, \cdots, b_{k-1})$ 是一个允许的 $(k-1)$- 正整数组，则存在无限多个素数 p, 使得 $p, p+b_1, \cdots, p+b_{k-1}$ 均为素数.

特别若 $(b_1, b_2, \cdots, b_{k-1})$ 是严紧而允许的, 则存在无穷多个类型 $(b_1, b_2, \cdots, b_{k-1})$ 的 k- 素数组.

在第六章 6.1 节我将考虑 Dickson 的一个猜想, 这个猜想是说在某些条件下一些线性多项式对同一自变量值可同时取素数值. Schinzel 和 Sierpiński(1958) 对此猜想作了透彻的研究. 而 k- 素数组的猜想是说：若 $(b_1, b_2, \cdots, b_{k-1})$ 是允许的，则多项式 $X, X+b_1, \cdots, X+b_{k-1}$ 可以无穷次地同时取素数值.

在证明 k- 素数组猜想之前需要证明孪生素数猜想. 许多致力于此项研究的人 (包括 Erdös) 都相信 k- 素数组猜想是正确的. 但是在现阶段，相信或不相信此猜想均纯粹是情绪所致.

正方的论点 一般来说, 人们相信孪生素数猜想正确. 既然如此，为什么 k- 素数组猜想对 $k > 2$ 不成立呢？人们的感觉是：这些问题对于每个 $k \geqslant 2$ 的难度是一样的，孪生素数猜想一旦被证明，其方法也可用来证明更一般的 k- 素数组猜想. “素数之家”

是好客的，它有容乃大到足以接纳孪生素数对，3- 素数组，4- 素数组，$\cdots$ 以及一切合法的素数族.

反方的论点 没有看到或摸到的东西是不存在的. 没有人见过允许的 $10^{10^{10}}$- 素数组. 这个猜想令人瞠目结舌，绝对没有支持 k- 素数组猜想的证据. 比较科学的依据是 Hensley 和 Richards 如下漂亮结果:

Hardy 和 Littlewood 猜想 (4.1H) 和 k- 素数组猜想不能同时正确.

证明 如果 k- 素数组猜想成立，我们来证 $\rho^*(x) \leqslant \rho(x)$. 由此得出对所有 $x > 1$, 均有 $\rho^*(x) = \rho(x)$.

令 $\rho^*(x) = k$, 于是存在允许的 $(k-1)$- 整数组 $(b_1, b_2, \cdots, b_{k-1})$, $b_{k-1} < x$, 由 k- 素数猜想，存在无穷多个素数 p, 使得 $p, p + b_1, \cdots, p+b_{k-1}$ 均为素数. 注意 $p-1 < p < p+b_1 < \cdots < p+b_{k-1} \leqslant p - 1 + x$. 从而由 $\rho(x)$ 的定义知 $\rho(x) \geqslant k = \rho^*(x)$. 由已经提到的定理, 存在 x_0, 使得对每个 $x \geqslant x_0, \rho^*(x) > \pi(x)$. 所以对每个 x, 由 $\rho^*(x) \leqslant \rho(x)$ 可知有无穷多个 y, 使得 $\pi(x) < \rho(x) = \pi(x+y) - \pi(y)$. 而这就表明在 k- 素数组猜想成立之下，Hardy-Littlewood 猜想不成立. □

Golomb 于 1992 年发表一个关于 k- 素数组平移特性的猜想，它至今未能解决.

Golomb 猜想 *存在一个递增整数列 $1 \leqslant a_1 < a_2 < \cdots$ 和整数 $B \geqslant 1$, 使得对每个 $n \in \mathbb{Z}$, 在序列 $a_1 + n < a_2 + n < \cdots$ 中素数的个数均不超过 B.*

下面是一个有趣的例子：对每个 $n \in \mathbb{Z}$, 形如 $((2k)!)^3 + n$ 的

数中只有有限多个素数. 因为在 $n=0$ 或 $|n|\geqslant 2$ 时这显然成立. 而对 $n=\pm 1$, 则有

$$((2k)!)^3-1=[(2k)!-1][((2k)!)^2+(2k)!+1]$$

$$((2k)!)^3+1=[(2k)!+1][((2k)!)^2-(2k)!+1]$$

但是对这个序列, 找不到猜想中所说的界 B.

1995 年, Ford 对下面定理给了一个漂亮的证明.

k- 素数组猜想和 Golomb 猜想不能同时成立.

证明 假设序列 $A=(a_i)_{i\geqslant 1}$ 和 $B\geqslant 1$ 满足 Golomb 猜想所述条件, 则如前所述, 存在常数 $c>0$ 使得对每个 $l\geqslant 2$,

$$\prod_{p\leqslant l}\left(1-\frac{1}{p}\right)>\frac{c}{\lg l}$$

取 l 使 $cl/\lg l>B$. 现在令 $A_l=\{a_1,a_2,\cdots,a_l\}$,$E_2=A_l\setminus(A_l\cap C)$, 其中 C 是奇数全体或偶数全体, 使得 $\#(A_l\cap C)$ 最小. 于是 $\#(A_l\cap C)\leqslant l/2$, 而 $\#(E_2)\geqslant l(1-1/2)$. 根据定义, E_2 中没有元素在 C 之中.

又令 $E_3=E_2\setminus(E_2\cap C')$, 其中 C' 是整数模 3 的一个同余类, 使得 $\#(E_2\cap C')$ 最小. 于是 $\#(E_2\cap C')\leqslant\#(E_2)/3$ 而

$$\#(E_3)\geqslant\#(E_2)\left(1-\frac{1}{3}\right)\geqslant l\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)$$

并且 E_3 中没有元素属于 C'. 继续下去 (对所有素数 $p\leqslant l$), 最后得到一个集合 E^*, 使得

$$\#(E^*)\geqslant l\prod_{p\leqslant l}\left(1-\frac{1}{p}\right)>\frac{cl}{\lg l}>B$$

由定义 $\#(E^*)<l$, 并且对每个素数 $q\leqslant\#(E^*)<l$,$\{b\mid b\in E^*\}$ 的模 q 同余类集合是模 q 所有同余类集合的真子集. 从而 E^* 是

允许集合. 根据 k- 素数组猜想, 存在无穷多素数 p, 使得 p 和 $p+b(b\in E^*)$ 均为素数. 对每个这样的 $p,\{a_i+p\mid i\geqslant 1\}$ 中均包括多于 B 个素数. 这导致矛盾. □

A.Granville 在 1989 年的信中告诉我, 对于多项式 X^2+X+c k-素数组猜想有如下的推论. (见 Mollin 1997), 令 $f(X)=aX^2+bX+c$, 其中 $a\geqslant b$. 现在假设 $2\mid a+b$, 并且 a 的每个奇素因子 q 都是 b 的因子.

若 k- 素数组猜想成立, 则对每个 $M>1$, 存在无穷多 $n\geqslant 1$, 使得 $f(0)+n,f(1)+n,\cdots,f(M)+n$ 均是素数. 用第三章 3.3C 的术语这可以说成: 平移多项式 $g_n(X)=f(X)+n$ 的素数生成长度大于 M.

证明 令 $S=\{f(0),f(1),\cdots,f(M)\}$. 现证 S 是允许集合. 首先 $f(0)\equiv f(1)\equiv\cdots\equiv f(M)\equiv c(\mathrm{mod}\ 2)$. 如果 q 为 a 的奇素数因子, 则 q 也是 b 的因子, 从而也有 $f(0)\equiv f(1)\equiv\cdots\equiv f(M)\equiv c\ (\mathrm{mod}\ q)$. 现设 q 为奇素数并且 q 不是 a 的因子. 取 u 和 a' 使得 $2u\equiv 1(\mathrm{mod}\ q),aa'\equiv 1(\mathrm{mod}\ q)$, 则对每个 s

$$as^2+bs+c\equiv a(s^2+a'bs)+c\equiv a(s+ua'b)^2+(c-a'u^2b^2)\quad(\mathrm{mod} q)$$

同余类 $at^2(\mathrm{mod}\ q)(t\in\mathbb{Z})$ 集合有 $(q+1)/2$ 个同余类, 所以存在 y 使得对每个 t, $y\not\equiv at^2(\mathrm{mod}\ q)$. 令 $z=y+(c-a'u^2b^2)$. 如果有 $s,0\leqslant s\leqslant M$ 使得 $z\equiv f(s)(\mathrm{mod}\ q)$, 则

$$y+(c-a'u^2b^2)\equiv a(s+ua'b)^2+(c-a'u^2b^2)(\mathrm{mod}\ q)$$

由此得出 $y\equiv a(s+ua'b)^2(\mathrm{mod}\ q)$, 这是不可能的. 这证明了 S 是允许集合. 于是由 k- 素数组猜想可知存在无穷多个 n, 使得 $g_n(X)=f(X)+n$ 在 $s=0,1\cdots,M$ 处均取素数值. □

4.5 算术级数中的素数

4.5A 存在无穷多个！

狄利克雷于 1837 年证明了一个经典的重要定理：

如果 $d \geqslant 2$ 和 $a \neq 0$ 均为整数，并且 d 和 a 是互素的，则在算术级数

$$a, a+d, a+2d, a+3d, \cdots$$

中包含无穷多个素数.

这个定理的许多特殊情况早就知道，包括欧几里得定理 ($a = 1, d = 2$). 而对 $d = 4$ 或 $6, a = -1$ 的情形可以用类似于欧几里得的方法证明. 利用二次剩余的简单性质，不难证明以下一些算术级数中均包含无穷多个素数.

$$d = 4, a = 1$$

$$d = 6, a = 1$$

$$d = 3, a = 1$$

$$d = 8, a = 3, 5 \text{ 或 } 7 \quad (\text{这也包含}d = 4\text{的算术级数})$$

$$d = 12, a = 5, 7 \text{ 或 } 11 \quad (\text{这也包含}d = 6\text{的算术级数})$$

对于 $d = 8, 16, \cdots$ 或更一般地 $d = 2^r$ 而 $a = 1$, 有一个简单的证明. 考虑 $f(N)$, 其中

$$f(X) = X^{2^{r-1}} + 1, \quad N = 2p_1p_2\cdots p_n$$

而每个素数 $p_i \equiv 1 (\bmod 2^r)$, 然后用费马小定理. 根据这个提示，读者自己会找到证明.

当 $a=\pm1$ 时，对于任何 d 都有初等证明，但是证明并不简单，需要分圆多项式的一些基本性质.

Hasse 在《数论讲义》一书 (Varlesungen über Zahlentheorie, 已有斯普林格出版社的英译本) 中对于狄利克雷定理的许多证明有详细的论述. Selberg 于 1949 年给出狄利克雷定理的一个初等证明，其方法类似于他对素数定理的初等证明.

对于狄利克雷定理， de la Vallée Poussin 给出如下的加性密度结果. 对于上述的 a 和 d, 以及 $x\geqslant 1$, 令

$$\pi_{d,a}(x)=\#\{\text{素数 } p\leqslant x \mid p\equiv a(\text{mod } d)\}$$

则

$$\pi_{d,a}(x)\sim\frac{1}{\varphi(d)}\cdot\frac{x}{\lg x}$$

注意右边与满足 $\gcd(a,d)=1$ 的 a 无关. 由此可知

$$\lim_{x\to\infty}\frac{\pi_{d,a}(x)}{\pi(x)}=\frac{1}{\varphi(d)}$$

这可以说成：算术级数 $\{a+kd \mid k\geqslant 1\}$ 中的素数组成的集合 (对于全体素数组成的集合) 具有自然密度 $1/\varphi(d)$.

虽然 $\pi_{d,a}(x)$ 的渐近性状对每个 $a(1\leqslant a\leqslant d,\gcd(a,d)=1)$ 是一样的，切比雪夫在 1853 年就发现对较小的 $x,\pi_{3,1}(x)<\pi_{3,2}(x),\pi_{4,1}(x)<\pi_{4,3}(x)$. 换句话说, 一直到不太大的 x, 形如 $3k+2$ 的素数多于形如 $3k+1$ 的素数 (同样地，形如 $4k+3$ 的素数多于形如 $4k+1$ 的素数). 这些不等式是否对所有 x 均对？情形与不等式 $\pi(x)<Li(x)$ 有些类似. 也像 Littlewood 定理一样，可以证明这些不等式有无穷多个情况是不对的. Leech 在 1957 年算出 $x_1=26861$ 是使 $\pi_{4,1}(x)>\pi_{4,3}(x)$ 成立的最小素数. Bays 和 Hudson(1978) 发现 $x_1=608981813029$ 是使 $\pi_{3,1}(x)>\pi_{3,2}(x)$ 成立的最小素数.

1977 年，Hudson 给出计算 $\pi_{d,a}(x)$(算术级数 $\{a+kd \mid k \geqslant 0\}$ 中小于 x 的素数个数) 的一个公式，类似于 $\pi(x)$ 的 Meissel 公式. Hudson 和 Brauer 在同一年还详细地研究了特殊算术级数 $4k \pm 1$ 和 $6k \pm 1$.

以下记 $\{p_n\}_{n \geqslant 1}$ 为全体素数的递增序列. 利用精细的解析方法，Shiu 在博士论文 (1996) 中证明了关于算术级数中相邻素数的如下定理 (还可见他 2000 年的文章)：

设 a 和 d 是互素的自然数，$1 \leqslant a < d$, 则存在正实数 x_0 和 C(均依赖于 a 和 d), 使得对每个实数 $x > x_0$, 均有 $n \geqslant 1$ 和

$$k \geqslant C\left[\frac{\log_2 x \log_4 x}{(\log_3 x)^2}\right]^{1/\varphi(d)}$$

满足 $p_{n+k} \leqslant x$ 并且 $p_{n+1} \equiv p_{n+2} \equiv \cdots \equiv p_{n+k} \equiv a (\mathrm{mod}\ d)$

这表明：每个可允许的算术级数均包含任意长的相邻素数序列. 这是因为当 x 趋于无穷时，k 也趋于无穷. 但这并不是说这些相邻素数本身也形成算术级数.

4.5B 算术级数中最小素数

设 $d \geqslant 2$ 和 $a \geqslant 1$ 彼此互素. 以 $p(d,a)$ 表示算术级数 $\{a+kd \mid k \geqslant 0\}$ 当中的最小素数. 能否给出 $p(d,a)$ 的一个只依赖于 a 和 d 的上界？

令 $p(d) = \max\{p(d,a) \mid 1 \leqslant a < d, \gcd(a,d) = 1\}$ 能否给出 $p(d)$ 的一个只依赖于 d 的上界，能否给出 $p(d)$ 的下界？

下面是 Linnik 1944 年一个定理，它是解析数论中最深刻的结果之一.

存在 $d_0 \geqslant 2$ 和 $L > 1$, 使得对每个 $d \geqslant d_0, p(d) < d^L$.

绝对常数 L 叫作 Linnik 常数，它是可有效计算的. 一个重要的事情是计算 L 的值. 潘承洞第一个计算了这个常数，在 1957 年

得到 $L \leqslant 5448$. 随后有一系列文章使这个估计不断地改进.

记录

Heath-Brown (1992) 证明了 $L \leqslant 5.5$, 优于陈景润和刘建明 (1989) 的 $L \leqslant 13.5$. 在这之前的工作还有陈景润 (1965), Jutila (1977), Graham (1981).

Schinzel 和 Sierpiński(1958) 和 Kanold(1963) 猜想 L=2, 即对充分大的 $d \geqslant 2$,$p(d) < d^2$. 更明确地说, 若 $1 \leqslant a < d, \gcd(a, d) = 1$, 则在 $a, a+d, a+2d, \cdots, a+(d-1)d$ 当中必有素数.

Heath-Brown 于 1978 年猜想 $p(d) \leqslant Cd(\lg d)^2$, 而 Wagstaff 基于经验在 1979 年认为 $p(d) \sim \varphi(d)(\lg d)^2$

关于 $p(d)$ 的下界, 我首先要指出 Schatunowsky(1893) 的下面结果, Wolfskehl 于 1901 年又独立地证明.

$d=30$ 是具有下列性质的最大整数: 若 $1 \leqslant a < d$, $\gcd(a, d) = 1$, 则 $a=1$ 或者 a 为素数.

证明是初等的, 可见 Landau 的书《素数》 (Primzahlen 1909) 第 229 页. 由此即知当 $d > 30$ 时 $p(d) > d+1$.

由素数定理可得到: 对每个 $\varepsilon > 0$ 和充分大的 d, 均有

$$p(d) > (1-\varepsilon)\varphi(d) \lg d$$

由此可得

$$\liminf \frac{p(d)}{\varphi(d) \lg d} \geqslant 1$$

1980 年 Pomerance 证明了更强的结果

$$\liminf \frac{p(d)}{\varphi(d)\lg d} \geqslant \mathrm{e}^{\gamma} = 1.78107\cdots$$

其中 γ 是欧拉常数. 另一方面, 以 Q 表示具有多于 $\exp(\log_2 d/\log_3 d)$ 个不同素因子的整数 $d \geqslant 2$ 所组成的集合, 则对 Q 以外的每个 d

$$\liminf \frac{p(d)}{\varphi(d)\lg d} \times t_d \geqslant \mathrm{e}^{\gamma}$$

其中

$$t_d = \frac{(\log_3 d)^2}{(\log_2 d)(\log_4 d)}$$

注意 $\lim\limits_{d\to\infty} t_d = 0$[⑧]. 特别地, 全体 $p(d)/(\varphi(d)\lg d)$ 组成无界集合.

对于这个问题, Prachar 和 Schinzel 在 1961 和 1962 年也得到以下相关结果.

注意集合 Q 的密度为零, 这是因为 d 的不同素因子个数的平均值为 $\log_2 d$.

1990 年, Granville 和 Pomerance 猜想: 对于 $d \geqslant 2$ 和某个常数 $C > 0$, 有

$$p(d) \geqslant C\varphi(d)(\lg d)^2$$

4.5C 素数组成算术级数

现在考虑如下的问题: 是否对每个 $k \geqslant 3$ 均存在 k 个素数 $p_1 < p_2 < \cdots < p_k$ 使得它们形成算术级数, 即 $p_2 - p_1 = p_3 - p_2 = \cdots = p_k - p_{k-1}$.

1939 年, van der Corput 证明了: 有无穷多个 3- 素数组是算术级数 (见 4.6 节).1944 年, Chowla 又证明了此事, 而 Heath-Brown 于 1985 年由更一般的定理又推出这个结果.

---

⑧ 事实上, $t_d = 2(\log_3 2)^2$ 为常数 —— 译者注.

不难给出 4 个 (或者更多) 素数形成算术级数的例子. 但是是否对每个 $k \geqslant 4$, 均存在无穷多个 k- 素数组形成算术级数？这个问题至今未解决.

先考查 $k=4$ 的情形，从中可知这个问题有多么困难. 目前最好的结果是 Heath-Brown 给出的. 他在 1981 年证明了：存在无穷多个 $\{a_1, a_2, a_3, a_4\}$ 形成算术级数，其中 3 个 a_i 为素数，而另一个是至多两个 (不必不同) 素数的乘积.

人们猜想对每个 $k>3$, 至少存在 k 个素数形成算术级数.

由很长的素数列形成算术级数，这方面有许多计算结果.

记录

目前所知形成算术级数的素数列最长为 22, 其中最小的素数为 $p=11410337850553$. 而公差为 $d=4609098694200$, 这是在 1993 年 3 月 17 日发现的 (发表于 1995 年), 是由 P.Pritchard(澳大利亚，昆士兰， Griffith 大学) 指挥 60 多台计算机算出来的. 这是一个真正的国际合作项目，这个 22 项素数组成的算术级数是在挪威的 Bergen 找到的. 他们也得到许多由 21 个素数组成的算术级数.

在这之前的记录为 Young 和 Fry(1987, 20 项), Pritchard(1985, 19 项； 1982, 18 项) 和 Weintraub (1977, 17 项). 这种研究的计算量是很大的.

与此有关的是下面一个容易证明的结果，它由 M.Cantor 于 1861 年推出，书面见于 Dickson 《数论史》一书卷 I 的第 425 页.

设 $d \geqslant 2, a, a+d, \cdots, a+(n-1)d$ 是由素数组成的算术级数. q 是不超过 n 的最大素数，则或者 $\prod_{p \leqslant q} p \mid d$, 或者 $a=q$ 并且 $\prod_{p<q} p \mid d$.

证明 首先注意，若素数 p 不整除 d, 并且 $a, a+d, \cdots, a+(p-1)d$ 均为素数，则这 p 个数彼此模 p 互不同余，从而 p 恰好除尽其中的一个. 现在设 $\prod_{p \leqslant q} p$ 不整除 d, 则存在素数 $p \leqslant n$, 使得 $p \nmid d$. 取满足此条件的最小素数 p, 由前所述, 存在 $j(0 \leqslant j \leqslant p-1)$ 使得 $p \mid a+jd$. 于是 $p = a+jd$, 因为 $a+jd$ 为素数. 但是 a 也是素数. 如果 $a \neq a+jd$, 则由 p 的选取知 $a \mid d$, 从而 $a \mid p$, 于是 $a = p+jd$. 这就表明 $p = a$. 若 $p < q$, 则 $p \leqslant n-1$, 从而 $p \mid a+pd$, 于是 $p = a+pd = p(1+d)$, 这是不可能的. 所以证明了：若 $\prod_{p \leqslant q} p \nmid d$, 则 $q = a$ 并且 $\prod_{p<q} p \mid d$. □

拉格朗日曾证明了上述命题的一个特殊情形.

在这里我要请读者回忆：我们在第三章 3.2 节曾讨论过一个更困难的问题：寻求 p 个素数组成的算术级数，其首项为素数 p.

比这还要困难的一个问题为：是否有由相邻素数组成的算术级数，其项数可以任意大？

记录

由相邻素数组成的算术级数，目前得到的最大长度为 10 项. 其第一项为

$$\begin{aligned} p =& 100996972469714247637786655587969840329509324 6\\ &- 8919004180360341775890434170334888215906722971 9\end{aligned}$$

而公差为 210. 它是 M.Toplic 于 1998 年 3 月 2 日找到的，Toplic 是国际范围 100 多个参与者之一. 这项工作由 D. Dubner, T. Forbes, N. Lygeros, M. Mizony 和 P. Zimmermann 指挥. 在此之前的记录也是由“幸运儿” M. Toplic 于 1998 年 1 月 24 日找到的，共 9

项，公差为 210, 而最小素数是

$$
\begin{aligned}
p =& 99679432066701086484490653695853561638982364 08 \\
& -0991618395774048585529071475461114799677694651
\end{aligned}
$$

4.6 哥德巴赫著名猜想

哥德巴赫在 1742 年给欧拉的信中，表示他相信：

(G) *每个整数 $n > 5$ 均是三个素数之和.*

欧拉回信说，容易看出这等价于：

(G') *每个偶数 $2n \geqslant 4$ 均是两个素数之和.*

因为若 (G') 成立，而 $2n \geqslant 6$, 则 $2n-2=p+p'$, 其中 p 和 p' 为素数. 从而 $2n+1=3+p+p'$, 即 (G) 成立. 反之若 (G) 成立，则当 $2n \geqslant 4$ 时 $2n+2=p+p'+p''$, 其中 p, p', p'' 均为素数. 然后可知这三个素数中一定有一个 (比如说是 p'') 为 2. 于是 $2n=p+p'$.

注意 (G') 对无穷多个偶数 $2p=p+p$ 是对的 (p 为所有素数).

一个有关的但是比较弱的问题是：是否每个大于 5 的奇数均为三素数之和？这叫作奇哥德巴赫猜想. 由它可推出：每个大于 6 的整数均可表示成不超过 4 个素数之和.

在精细的解析方法和筛法研究出来之前，这些猜想的进展甚微. 虽然已经作了许多努力，这些问题至今仍未解决.

人们的努力分成三条主线，它们可以 (也许不适当) 用三个关键词来表达："渐近"，"殆素数"，"基".

(a) 渐近性命题是指对充分大整数均成立的命题.

这方面的第一个重要结果是 Hardy 和 Littlewood 在 1923 年的一个渐近定理. 用圆法和黎曼猜想的一个修改的形式，他们证明了存在 n_0, 使每个奇数 $n \geqslant n_0$ 均为三个素数之和.

后来在 1937 年，Vinogradov 不用黎曼猜想证明了上述结果. 1985 年 Heath-Brown 给出了另一个证明，但是常数 n_0 不是有效的.

Borodzkin 仔细研究了 Vinogradov 的证明, 在 1956 年给出 n_0 可取 $3^{3^{15}} \approx 10^{7000000}$.1989 年陈景润和王天泽得到 $n_0 = 10^{43000}$,1996 年他们又得到 $n_0 = 10^{7194}$. 但是这仍旧太大，不足以能使计算机来验证小于 n_0 的奇数.

1997 年， Deshouillers,Effinger,te Riele 和 Zinoview 解决了这个问题：每个大于 5 的奇整数均是三个素数之和，但是需要假设类似于黎曼猜想的一个猜想成立.

(b) 对于 $k \geqslant 1$, 不超过 k 个素数的乘积 (素因子可以相同) 叫作 k- 殆素数. 所有 k- 殆素数组成的集合表示成 P_k.

用殆素数的方式考虑问题是去证明存在 $h, k \geqslant 1$, 使得每个充分大的偶数都可表成一个 k- 殆素数与一个 h- 殆素数之和. 人们希望的当然是 k 和 h 均为 1.

在这个方向, 第一个结果是由 Brun(1919, C.R.Acad.Sci.Paris) 给出的：每个充分大的偶数都是两个 9- 殆素数之和. 利用不断改进的筛法，这个问题也不断进展. 1950 年 Selberg 证明了每个充分大的偶数都在集合 $P_2 + P_3$ 中，即是 P_2 中一个整数和 P_3 中一个整数之和. 1947 年 Rényi 证明了：存在整数 $k \geqslant 1$, 使得充分大的偶数均在 $P_1 + P_k$ 之中. 后来的工作是给出 k 的值.

目前最好的结果是陈景润给出的 (1966 年宣布，证明细节发表于 1973 年和 1978 年). 在他的著名文章中给出最接近于哥德巴

赫猜想的如下结果：

每个充分大的偶整数 $2n$ 都可表成 $2n = p + m$, 其中 p 为素数而 $m \in P_2$.

与此同时，陈景润还证明了一个“伴随”结果：存在无穷多个素数 p, 使得 $p + 2 \in P_2$. 这十分接近于孪生素数有无穷多的猜想. 用同样方法还可以证明：对每个偶数 $2k \geqslant 2$, 均有无穷多个素数 p, 使得 $p+2k \in P_2$. 所以 $2k$ 可以用无穷多种方式表示成 $m-p$, 其中 p 为素数，而 $m \in P_2$.

陈氏定理的证明可见 Halberstam 和 Richart 的书，也可见 Ross (1975) 给出的简化证明.

(c)　“基”方法始于 Schnirelmann(1930) 一个著名的定理，证明可见 Landau 的书 (1937) 或 Gelfond 和 Linnik 的书 (1965 年英译本)：

存在一个正整数 S, 使得每个充分大的整数都不超过 S 个素数之和.

由此可以推出，存在一个正整数 $S_0 \geqslant S$, 使得每个大于 1 的整数都是不超过 S_0 个素数之和.　S_0 叫作 Schnirelmann 常数. 哥德巴赫猜想可表示成：　$S_0 = 3$.

Khinchin 在他短小精练的书 (1947) 中对于 Schnirelmann 思想和数列密度用一章作了有趣和通俗易懂的介绍.

Schnirelmann 常数的有效决定方面有许多计算结果.

记录

目前最好估计 $S_0 \leqslant 6$ 是 Ramaré 于 1995 年给出的. 在此之前的最好结果是 Riesel 和 Vaugham (1983) 的 $S_0 \leqslant 19$.

1949 年， Richert 证明了 Schnirelmann 定理的一个类比：每个整数 $n > 6$ 均可表成不同素数之和．请读者注意： Schinzel 于 1959 年证明了哥德巴赫猜想可以推出 (从而等价于)：每个整数 $n > 17$ 都可表成恰好三个不同素数之和．所以 Richert 的结果为哥德巴赫猜想的一个推论.

(d) 表法个数.

现在讨论 $2n \geqslant 4$ 表成两个素数和表法个数 $r_2(2n)$. 在哥德巴赫猜想被证明之前， $r_2(2n)$ 可能为 0.

Hardy 和 Littlewood 于 1923 年给出下面的渐近公式. 他们的证明要假定黎曼猜想一个变化的形式，后来由 Vinogradov 去掉了这个假定

$$r_2(2n) \leqslant C\frac{2n}{(\lg 2n)^2}\lg\lg 2n$$

对于 $n > 2$, 以 $\pi^*(n)$ 表示满足 $n/2 \leqslant p \leqslant n-2$ 的素数 p 的个数．显然 $r_2(n) \leqslant \pi^*(n)$.Deshouillers,Granville,Narkiewicz 和 Pomerance 于 1993 年证明了 $n = 210$ 是使 $r_2(n) = \pi^*(n)$ 的最大整数.

1985 年， Powell 在数学期刊 *MathematicsMagazine* 中提出一个问题：是否有初等方法，证明对每个 $k > 0$ 均存在无穷多偶数 $2n$ 使得 $r_2(2n) > k$ ？ Finn 和 Frohliger 于 1986 年给出一个解法．下面是我给出的证明．只用到以下事实：在不超过 x 的整数中至少有 $x/(2\lg x)$ 个素数，这是比切比雪夫不等式要弱的命题.

证明 取 x 使 $x/(2\lg x) > \sqrt{2kx}+1$. 以 P 为不超过 x 的所有奇素数组成的集合．则 $|P| \geqslant x/(2\lg x)$. 又令 $P_2 = \{(p,q) \mid p,q \in P, p < q\}$, 则

$$|P_2| \geqslant \frac{1}{2}\cdot\frac{x}{2\lg x}\Big(\frac{x}{2\lg x}-1\Big)$$

现在令 $f(p,q)=p+q$, 则 f 的像是不超过 $2x-2$ 的偶数，所以 f 的像集合最多有 $x-4$ 个元素. 于是存在 $n\leqslant 2x-2$, 使得集合 $\{(p,q)\in P_2 \mid p+q=n\}$ 的元素个数至少为

$$\frac{P_2}{x-4}>\frac{1}{2x}\Big(\frac{x}{2\lg x}-1\Big)^2>k$$

(e) 例外集合.

对每个 $x\geqslant 4$, 令

$$G'(x)=\#\{2n \mid 2n\leqslant x, 2n\text{不为两个素数之和}\}$$

Van der Corput(1937),Estermann(1938) 和 Tschudakoff(1938) 各自独立地证明了 $\lim G'(x)/x=0$, 并且事实上对每个 $\alpha>0$ 均有 $G'(x)=O(x/(\lg x)^\alpha)$.Heath-Brown 于 1985 年给出另一个证明.

在这方面的最好结果是 Montgomery 和 Vaugham(1975) 在一篇深刻论文中给出的：存在有效可计算的 $\alpha(0<\alpha<1)$, 使得对每个充分大的 x,$G'(x)<x^{1-\alpha}$.1980 年，陈景润和潘承洞证明了 α 可取为 1/100, 而陈景润 (1983) 又改成 $\alpha=1/25$(潘承洞也独立地证明此结果).

关于哥德巴赫猜想的数值结果，下面是目前的记录.

记录

(1) 先考虑三个素数问题. Saouter 于 1998 年验证了每个小于 10^{20} 的奇数均不超过三个素数之和.

(2) 对于哥德巴赫猜想. Deshouilliers,te Riele 和 Saouter 于 1998 年验证了哥德巴赫猜想对于 10^{14} 以内的偶数成立. Richstein(2001) 又把计算扩大到 4×10^{14}. 最近 T.Oliveira e Silva 进一步验证到 8×10^{15}, 并且还在继续他的计算工作.

在此之前， Sinisalo(1993) 验证到 4×10^{11},Granville,van de Lune 和 te Riele(1989) 验证到 2×10^{10}.

哥德巴赫问题的一个变异

这次的问题是把每个奇数表成一个素数与 2 的一个方幂之和. 从而它既像哥德巴赫问题，又像孪生素数问题. 这个问题由 Prince A.de Polignac 提出. 他在 1849 年宣称：每个奇自然数均为一个素数和一个 2 的方幂之和. 但很快他发现自己的证明有错误，因为 959 就没有这种表示方法. 详见 Dickson 的《数论史》第 I 卷第 424 页.

于是仍需要研究集合 $A = \{p + 2^k \mid p\text{为素数}, k \geqslant 1\}$. 我这里只介绍一部分结果. Romanoff 于 1934 年证明了 A 具有正密度，即存在 $C > 0$, 使得对每个 $x \geqslant 1$,$\#\{m \in A \mid m \leqslant x\}/x > C$.

Erdös 于 1950 年研究了此问题. 首先由素数定理得到 $\#\{m \in A \mid m \leqslant x\} = O(x)$. 他还证明了存在由奇整数组成的一个算术级数，其中不包含任何形如 $p + 2^k \in A$ 的整数.

整数 $n = 7, 15, 21, 45, 75, 105$ 满足以下性质：对每个 $2^k < n, n - 2^k$ 均为素数. Erdös 猜想不再有正整数满足此性质. 令 $R(n) = \#\{(p, k) \mid p\text{为奇素数}, k \geqslant 1, p + 2^k = n\}$. Erdös 证明了存在 $C > 0$, 使得有无穷多个 n 满足 $R(n) > C \lg\lg n$.

4.7 拟素数和 Carmichael 数的分布

现在介绍拟素数和 Carmichael 数的分布结果.

4.7A 拟素数的分布

以 $P\pi(x)$ 表示不超过 x 的 (以 2 为基) 拟素数，而 $(\mathrm{psp})_1 <$

$(\mathrm{psp})_2 < \cdots < (\mathrm{psp})_n < \cdots$ 是由全体拟素数组成的递增数列. 1949 和 1950 年， Erdös 给出如下估计：存在 $C>0$, 使对充分大的 x

$$C \lg x < P\pi(x) < \frac{x}{\mathrm{e}^{\frac{1}{3}(\lg x)^{1/4}}}$$

利用第二章 2.8 节介绍的 Lehmer 方法来产生无穷多个以 2 为基的拟素数，从而容易证明更明确的结果：若 $x \geqslant 341$, 则 $0.171 \lg x \leqslant P\pi(x)$. 我马上要指出，这些结果后来有很大改进.

由这些估计可推出

$$\sum_{n=1}^{\infty} \frac{1}{(\mathrm{psp})_n}$$

是收敛的 (这首先由 Szymiczek 于 1967 年证明), 而

$$\sum_{n=1}^{\infty} \frac{1}{\lg(\mathrm{psp})_n}$$

是发散的 (这首先由 Mąkowski 于 1974 年证明).

为了计算拟素数、欧拉拟素数和强拟素数 (以任意 $a \geqslant 2$ 为基) 的个数，较方便的是采用以下记号

$$\begin{array}{ll} P\pi_a(x) = \#\{n \mid 1 \leqslant n \leqslant x,\ n\text{为 psp}(a)\}, & P\pi(x) = P\pi_2(x) \\ EP\pi_a(x) = \#\{n \mid 1 \leqslant n \leqslant x,\ n\text{为 epsp}(a)\}, & EP\pi(x) = EP\pi_2(x) \\ SP\pi_a(x) = \#\{n \mid 1 \leqslant n \leqslant x,\ n\text{为 spsp}(a)\}, & SP\pi(x) = SP\pi_2(x) \end{array}$$

显然 $SP\pi_a(x) \leqslant EP\pi_a(x) \leqslant P\pi_a(x)$.

现在考虑这些函数的上下界估计.

对于 $P\pi(x)$ 的上界， Pomerance 改进了 Erdös(1956) 结果，于 1981 年证明了：对所有大 x 值，

$$P\pi(x) \leqslant \frac{x}{l(x)^{1/2}}$$

其中

$$l(x) = e^{\lg x \lg\lg\lg x / \lg\lg x}$$

对任何基 $a \geqslant 2$, 这也是 $P\pi_a(x)$ 的上界.

对于下界，目前最好的结果是 Pomerance 于 1982 年给出的 (见他文章中的注记 3)

$$e^{(\lg x)^\alpha} \leqslant SP\pi_a(x)$$

其中 $\alpha = 5/14$. 利用 Lehmer 产生对基 2 拟素数的初等方法，可以得到一个明显的但是较弱的下界 $0.171 \lg x \leqslant P\pi(x)$.

由拟素数表可建议：对每个 $x \geqslant 170$, 在 x 和 $2x$ 之间必存在拟素数. 但这并未被证明. 这方面还有 Rotkiewicz(1965) 如下结果：

对每个整数 $n > 19$, 在 n 和 n^2 之间均存在拟素数. 进而，对每个 $\varepsilon > 0$ 均存在 $x_0 = x_0(\varepsilon) > 0$, 使得当 $x > x_0$ 时在 x 和 $x^{1+\varepsilon}$ 之间均存在拟素数.

关于算术级数中的拟素数， Rotkiewicz 在 1963 和 1967 年证明了：

若 $a, d \geqslant 1, \gcd(a, d) = 1$ 则在算术级数 $\{a + kd \mid k \geqslant 1\}$ 中有无穷多个拟素数.

以 $\mathrm{psp}(d, a)$ 表示在上述算术级数中的最小拟素数. Rotkiewicz 于 1972 年证明了：

对每个 $\varepsilon > 0$ 和充分大的 d, 均有 $\lg \mathrm{psp}(d, a) < d^{4L^2+L+\varepsilon}$, 其中 L 是 Linnik 常数 (见 4.4 节).

上述结果由 van der Poorten 和 Rotkiewicz 在 1980 年加以推广：若 $a, d \geqslant 1, \gcd(a, d) = 1$, 则对每个 $b \geqslant 2$ 算术级数 $\{a + kd \mid k \geqslant 1\}$ 中包含无穷多个以 b 为基的奇的强拟素数.

4.7B Carmichael 数分布

现在谈 Carmichael 数的分布. 以 $CN(x)$ 表示不超过 x 的 Carmichael 数的个数.

先讨论 $CN(x)$ 的上界. 1956 年 Erdös 证明了: 存在常数 $\alpha > 1/2$, 使得对每个充分大的 x

$$CN(x) \leqslant \frac{x}{l(x)^{\alpha}}$$

其中 $l(x)$ 定义见 4.7A 小节.

Pomerance, Selfridge 和 Wagstaff 在 1980 年将此结果改进为: 对每个 $\varepsilon > 0$, 均存在 $x_0(\varepsilon) > 0$, 使得当 $x \geqslant x_0(\varepsilon)$ 时

$$CN(x) \leqslant \frac{x}{l(x)^{1-\varepsilon}}$$

求 $CN(x)$ 下界是困难的. Alford,Granville 和 Pomerance(1994) 在证明存在无穷多 Carmichael 数的时候, 也给出对充分大 x, 有 $CN(x) \geqslant x^{2/7}$.Pomerance,Selfridge 和 Wagstaff 猜想对充分大 x, 应当有 $CN(x) \geqslant x/l(x)^{1-\varepsilon}$.Granville 1992 年文章是上述诸结果的一个通俗介绍.

现在谈关于拟素数和 Carmichael 数的表. 1938 年 Poulet 决定出 10^8 以内 (以 2 为基) 的全部 (奇) 拟素数, 其中也散见一些 Carmichael 数. Swift 于 1975 年造了 10^9 以内的 Carmichael 数表, 而 Yorinaga 于 1979 年扩大到 10^{10}.

Pomerance,Selfridge 和 Wagstaff(1980) 的表给出 25×10^9 以内的拟素数、欧拉拟素数、 (以 2 为基) 强拟素数和 Carmichael 数. Pinch 分别在 1992 年和 2000 年把此表扩大到 10^{12} 和 10^{13}(见表 4.5).

1990 年, Jaeschke 把 Carmichael 数的表扩大到 10^{12}.Pinch 分别于 1993 年和 1998 年将此表扩大到 10^{15} 和 10^{16}(并对原表作了

修订). 表 4.6 给出 10^M 以内 ($3 \leqslant M \leqslant 16$) 具有 k 个不同素因子的 Carmichael 数的个数.

表 4.5　$P\pi(x), EP\pi(x), SP\pi(x)$和 $CN(x)$

x	$P\pi(x)$	$EP\pi(x)$	$SP\pi(x)$	$CN(x)$
10^3	3	1	0	1
10^4	22	12	5	7
10^5	78	36	16	16
10^6	245	114	46	43
10^7	750	375	162	105
10^8	2057	1071	488	255
10^9	5597	2939	1282	646
10^{10}	14884	7706	3291	1547
25×10^9	21853	11347	4842	2163
10^{11}	38975	20417	8607	3605
10^{12}	101629	53332	22412	8241
10^{13}	264239	124882	58897	19279

表 4.6　Carmichael 数的素因子个数

M	k								总数
	3	4	5	6	7	8	9	10	
3	1	0	0	0	0	0	0	0	1
4	7	0	0	0	0	0	0	0	7
5	12	4	0	0	0	0	0	0	16
6	23	19	1	0	0	0	0	0	43
7	47	55	3	0	0	0	0	0	105
8	84	144	27	0	0	0	0	0	255
9	172	314	146	14	0	0	0	0	646
10	335	619	492	99	2	0	0	0	1547
11	590	1179	1336	459	41	0	0	0	3605
12	1000	2102	3156	1714	262	7	0	0	8241
13	1858	3639	7082	5270	1340	89	1	0	19279
14	3284	6042	14938	14401	5359	655	27	0	44706
15	6083	9938	29282	36907	19210	3622	170	0	105212
16	10816	16202	55012	86696	60150	16348	1436	23	246683

Pinch 还制造了关于 Carmichael 数的下述表格:

(1) 对于 $3 \leqslant k \leqslant 20$, 具有 k 个素因子的最小 Carmichael 数.

(2) 25×10^9 以内在模 5, 7, 11, 12 的每个同余类中, 和 10^M 以内 $(11 \leqslant M \leqslant 16)$Carmichael 数的个数.

(3) 每个素数 $p \leqslant 97$ 成为 Carmichael 数的因子 (或最小因子) 的频率.

4.7C Lucas 拟素数的分布

我们在第二章 2.10 节讲过 Lucas 拟素数. 对于非零整数 P 和 Q, 记 $D = P^2 - 4Q$, 则 Lucas 序列定义为

$$U_0 = 0,\ U_1 = 1,\ U_n = PU_{n-1} - QU_{n-2} \quad (n \geqslant 2)$$

而与 D 互素的合成数 n 叫作 Lucas 拟素数 (对于参数 (P,Q)), 是指 $n \mid U_{D-(D|n)}$, 其中 $(D|n)$ 是雅可比符号.

由于 Lucas 拟素数是近来提出的概念, 这种数的分布结果不多. 这里叙述的主要结果来源于第二章所引的 Baillie 和 Wagstaff (1980) 的文章.

以 $L\pi(x)$ 表示不超过 x 的 Lucas 拟素数 (对于参数 (P,Q)) 的个数. 则当 x 充分大时

$$L\pi(x) < \frac{x}{\mathrm{e}^{Cs(x)}}$$

其中 $C > 0$ 为常数, 而 $s(x) = (\lg\lg\lg x)^{1/2}$.

由此推出 (类似于 Szymiczek 关于拟素数的结果): 对每个给定的参数 (P,Q), $\sum(1/U_n)$ 收敛 (对参数 (P,Q) 的所有 Lucas 拟素数求和).

另一方面, Erdös,Kiss 和 Sárközy(1988) 证明了: 存在常数 $C > 0$, 使得对每个非退化 Lucas 序列和充分大的 x, 均有 $L\pi(x) > \exp\{(\lg x)^C\}$.

类似地, 对于不超过 x 的 (参数为 (P, Q)) 强 Lucas 拟素数个数 $SL\pi(x)$(见第二章 2.10 节定义) 有下界：对充分大的 x，$SL\pi(x) > C'\lg x$, 其中 $C' > 0$ 为常数.



第五章　哪些特殊的素数被研究？

我们已经见过一些特殊类型的素数，比如是费马数或 Mersenne 数的素数 (见第二章). 现在要讨论其他几类素数，包括正规素数、Sophie Germain 素数、Wieferich 素数、Wilson 素数、全 1 素数和二阶线性递归序列中的素数.

正规素数、Sophie Germain 素数和 Wieferich 素数直接来源于证明费马猜想，有兴趣的读者可参阅我的书《关于费马大定理的十三讲》，书中对这些事情有更详细的介绍. 特别地，那里有大量参考文献，包括在本书未能列入的许多经典文献.

5.1　正规素数

正规素数是在 Kummer 研究费马猜想时出现的. 他于 1847 年给刘维尔 (Liouville) 的信中，说他对于满足两个条件的所有素数 p 证明了费马猜想. 事实上，他所证明的是：对于满足这些条件的素数 p, 不存在非零整数 x, y, z, 使得 $x^p + y^p = z^p$. 然后他说："剩下的事情只是看是否所有素数都满足这些性质".

为了描述这些性质，我需要解释 Kummer 首次引进的一些概念. 设 p 为奇素数，而

$$\zeta = \zeta_p = \cos\frac{2\pi}{p} + \mathrm{i}\sin\frac{2\pi}{p}$$

是 p 次本原单位根. 由 $X^p - 1 = (X-1)(X^{p-1} + X^{p-2} + \cdots + X + 1)$ 和 $\zeta^p = 1, \zeta \neq 1$ 可知 $\zeta^{p-1} + \zeta^{p-2} + \cdots + \zeta + 1 = 0$. 所以 ζ^{p-1} 可

用 ζ 的低次幂表示. 令

$$K = \{a_0 + a_1\zeta + \cdots + a_{p-2}\zeta^{p-2} \mid a_i \in \mathbb{Q}\}$$

$$A = \{a_0 + a_1\zeta + \cdots + a_{p-2}\zeta^{p-2} \mid a_i \in \mathbb{Z}\}$$

则 K 为域, 叫作 p- 分圆域. 而 A 为环, 叫作 p- 分圆整数环. A 中的单位是可整除 1 的数 $\alpha \in A$, 即存在 $\beta \in A$ 使得 $\alpha\beta = 1$.A 中的元素 α 叫作分圆素数, 是指 α 不能表成 $\beta\gamma$, 使得 $\beta, \gamma \in A$ 但均不是单位.

我们称 p- 分圆整数环 A 是唯一分解的, 是指 A 是每个非零分圆整数均可表成分圆素数的乘积, 并且这种分解不计单位因子是唯一的. Kummer 在 1847 年就发现, 当 $p \leqslant 19$ 时 p- 分圆整数环 A 是唯一分解的, 但是对 $p = 23$ 则不然.

为了处理分解不唯一的情形, Kummer 引进"理想数"概念. 后来狄德金 (Dedekind) 考虑一些分圆整数集合, 叫作理想. 我假定读者熟悉理想的定义. 狄德金的理想更适合于具体描述 Kummer 的理想数, 所以用狄德金的理想来叙述 Kummer 结果更为方便. 一个素理想 P 是不为 (0) 和环 A 的理想, 并且若 P 为两个理想的乘积 IJ, 则 I 和 J 必有一个为 P.Kummer 证明了: 对每个素数 $p > 2$,p- 分圆整数环的每个理想 $(\neq (0), A)$ 都唯一表成素理想的乘积.

两个非零理想 I 和 J 是等价的, 是指存在非零分圆整数 $\alpha, \beta \in A$, 使得 $A\alpha \cdot I = A\beta \cdot J$. 理想的等价类集合是满足消去律的交换半群. Kummer 证明了这是有限集合, 所以它是群, 叫作理想类群. 此群中元素个数叫作类数, 表示成 $h = h(p)$, 这是非常重要的算术不变量.

分式理想和理想类概念以及类数的有限性是代数数域理论的核心内容. 除了目前分圆域之外, 我们曾经考虑过二次域的情形

(第三章 3.3B 节).

类数 $h(p)$ 为 1 恰好相当于 A 中每个理想都是主理想. 即有形式 $A\alpha(\alpha\in A)$. 所以 $h(p)=1$ 当且仅当 p- 分圆整数环 A 是唯一分解的. 从而 $h(p)$ 的大小可衡量与唯一分解性偏差的程度.

Kummer 研究出十分深刻的理论, 他给出计算 $h(p)$ 的具体公式, 对较小的 p 可计算 $h(p)$.

在费马猜想中 Kummer 需要 p 的一个性质: $p\nmid h(p)$. 后人把具有这个性质的素数 p 叫作正规素数.

Kummer 提到的第二个性质是与单位有关的. 他后来证明了这个性质被所有正规素数所满足. 这是另一个漂亮的结果, 现在称之为 Kummer 的单位定理.

Kummer 给出正规素数的一个判别方法: 奇素数 p 是正规的当且仅当 p 不能整除伯努利数 $B_2,B_4,B_6,\cdots,B_{p-3}$ 的所有分子 (伯努利数的定义见第四章 4.1A 节).

Kummer 用此决定了 163 以内的所有不正规素数, 他们为 37, 59, 67, 101, 103, 131, 149 和 157. 他希望有无穷多个正规素数. 大量数据显示这应该是对的, 但是这是一个十分困难的问题.

1964 年, Siegel 根据伯努利数模一个素数同余性的经验性假设, 得到正规素数在所有素数当中的密度为 $1/\sqrt{\mathrm{e}}\approx 61\%$. 另一方面, Jensen 于 1915 年令人惊奇地证明了不正规素数有无穷多个. 证明实际上相当容易, 只需要伯努利数的一些算术性质.

以 $\pi_{\mathrm{reg}}(x)$ 表示不超过 x 的正规素数的个数, 而

$$\pi_{\mathrm{ir}}(x)=\pi(x)-\pi_{\mathrm{reg}}(x)$$

对每个不正规素数 p, 称 $(p,2k)$ 为不正规数对是指 $2\leqslant 2k\leqslant p-3$ 并且 p 整除 B_{2k} 的分子. 而不正规数对 $(p,2k)$ 的个数叫作 p 的不正规指数, 表示成 $ii(p)$. 对于 $s\geqslant 1$, 以 $\pi_{iis}(x)$ 表示满足 $ii(p)=s$

的 x 以内素数 p 的个数.

记录

关于正规素数的最重要计算工作依时间次序有 Johnson (1975), Wagstaff (1978), Tanner 和 Wagstaff (1989) , Buhler, Crandall 和 Sompolski (1992), Buhler, Crandall, Ernvall 和 Metsänkylä (1993), 以及近来的 Buhler, Crandall, Ernvall, Metsänkylä 和 Shokrollahi (2001) 作出. 已经完全决定出 $N = 12 \times 10^{16}$ 以内全部不正规素数和它们的不正规指数. 下面是一些结果 (2 既不算是正规素数, 也不算是不正规素数) :

$$\begin{aligned}
\pi(N) &= 788060 \\
\pi_{\text{reg}}(N) &= 477616 \\
\pi_{\text{ir}}(N) &= 310443 \\
\pi_{ii1}(N) &= 239483 && \text{(最小的素数是37)} \\
\pi_{ii2}(N) &= 59710 && \text{(最小的素数是157)} \\
\pi_{ii3}(N) &= 9824 && \text{(最小的素数是491)} \\
\pi_{ii4}(N) &= 1282 && \text{(最小的素数是12613)} \\
\pi_{ii5}(N) &= 127 && \text{(最小的素数是78233)} \\
\pi_{ii6}(N) &= 13 && \text{(最小的素数是527377)} \\
\pi_{ii7}(N) &= 4 && \text{(最小的素数是3238481)} \\
\pi_{ii8}(N) &= 0 \ (\text{对} s \geqslant 8)
\end{aligned}$$

目前知道: 最大正规素数为 $p = 11999989$, 最长的连续正规素数列是以 17881 开始的 27 个素数. 最长的连续不正规素数列是以 670619 开始的 14 个素数.

"相邻" 不正规数对 $(p, 2k), (p, 2k+2)$ 目前只知道两个: $p = 491, 2k = 336$ 和 $p = 587, 2k = 90$. 没有发现不正规数对的连续三对 $(p, 2k), (p, 2k+2), (p, 2k+4)$.

对每个素数 $p \geqslant 11$,p 叫作 Wolstenholme 素数 (见第二章 2.2C 节), 是指 p 整除伯努利数 B_{p-3} 的分子 (即 $(p, p-3)$ 是不正规数对).

猜想存在素数具有任意大的不正规指数，但是未被证明.

由 Kummer 定理，Vandiver 的一个判别法和上面报告的计算结果可知，费马猜想对于 12×10^6 以内的素数指数 p 都是对的.

素数的正规性与数论的许多问题有关，它与费马猜想的联系已成为历史，因为费马猜想已被证明，其证明是 G. Frey, K. A. Ribet, J. P. Serre, A. Wiles 和 R. Taylor 合力的成就.

5.2 Sophie Germain 素数

我们在第二章讲述过 Mersenne 数的因子的欧拉判别法时已经见到过 Sophie Germain 素数. 让我们回忆：p 叫作 Sophie Germain 素数是指 p 和 $2p+1$ 均为素数. 这种素数是由 Sophie Germain 首先考虑的，她证明了如下美妙定理：

若 p 是 Sophie Germain 素数，则 $x^p + y^p = z^p$ 不存在整数解 (x, y, z) 使得 $p \nmid xyz$.

换句话说，对于 Sophie Germain 素数，费马猜想的“第一种情形”是正确的. 详细讨论可见我的书 (1979) 或者我更近的书 (1999).

人们认为存在无穷多个 Sophie Germain 素数，但是它的证明会和证明无穷多对孪生素数的存在性具有同样的困难程度.

这里我想更详细解释一下费马猜想第一种情形与诸如 Sophie Germain 素数之间的关系.

Sophie Germain 定理被勒让德，后来被 Dénes(1951) 以及近来被 Fee 和 Granville(1991) 加以推广.

现在谈对不超过 x 的 Sophie Germain 素数个数的估计，更一

般地，设 $a, d \geqslant 1$,ad 为偶数，$\gcd(a, d) = 1$. 对每个 $x \geqslant 1$, 令

$$S_{d,a}(x) = \#\{素数p \leqslant x \mid a + pd为素数\}$$

对于 $a = 1, d = 2$,$S_{2,1}(x)$ 即是不超过 x 的 Sophie Germain 素数的个数.

利用估计小于 x 的孪生素数对个数的 Brun 筛法，可给出类似的界

$$S_{d,a}(x) < \frac{Cx}{(\lg x)^2}$$

由素数定理可知

$$\lim_{x \to \infty} \frac{S_{d,a}(x)}{\pi(x)} = 0$$

所以我们有理由说：使 p 和 $a + pd$ 均为素数的 p 所成集合在全体素数组成的集合中密度为零. 特别地，Sophie Germain 素数集以及孪生素数集合均应密度为零. 1980 年，Powell 不用筛法证明了上述结果 (见表 5.1).

表 5.1　不超过 x的 Sophie Germain 素数个数 $S_{2,1}(x)$

x	$S_{2,1}(x)$
10^3	37
10^4	190
10^5	1171
10^6	7746
10^7	56032
10^8	423140
10^9	3308859
10^{10}	26569515

后两行是由 W.Keller 和 C.F.Kerchner 彼此独立地计算出的. 至今已经发现许多大的 Sophie Germain 素数 (见表 5.2).

与 Sophie Germain 素数有密切联系的是如下一个题目. 素数递增序列 $q_1 < q_2 < \cdots < q_k$ 叫作长为 k 的第一类 (第二类)Cunningham链, 是指对每个 $i = 1, 2, \cdots, k-1$, 均有 $q_{i+1} = 2q_i + 1(q_{i+1} = 2q_i - 1)$. 所以在第一类 Cunningham 链中的素数均为 Sophie Germain 素数. 目前不知道是否对每个 $k > 2$, 均存在长度大于或等于 k 的 (第一类或第二类) Cunningham 链.

表 5.2 已知的大 Sophie Germain 素数

Sophie Germain 素数	位数	发现者	年份
$2540041185 \times 2^{114729} - 1$	34547	D.Unerbakke, G.Woltman and Y.Gallot	2003
$18912879 \times 2^{98395} - 1$	29628	M.J.Angel, D.Augutin, P.Jobling and Y.Gallot	2002
$1213822389 \times 2^{81131} - 1$	24432	M.J.Angel, D.Augustin, P.Jobling and Y.Gallot	2002
$109433307 \times 2^{66452} - 1$	20013	D.Underbakke, P.Jobling and Y.Gallot	2001
$984798015 \times 2^{66444} - 1$	20011	D.Underbakke, P.Jobling and Y.Gallot	2001
$3714089895285 \times 2^{60000} - 1$	18075	K.-H.Indlekofer, A.Járai and H.-G.Wassing	2000
$37561665 \times 2^{34090} - 1$	10270	C.Abraham	2003
$831264873 \times 2^{33539} - 1$	10106	K.Schoenberger and Y.Gallot	2003
$168851511 \times 2^{33250} - 1$	10018	D.O.Kremelberg and Y.Gallot	2003
$918522549 \times 2^{33216} - 1$	10008	J.A.Rouse and Y.Gallot	2003

记录

目前已知的第一类 Cunningham 链的最大长度为 14, 其最小素数为 14374829422532838039. 目前已知的第二类 Cunningham 链的最大长度为 16, 其最小素数为 3203000719597029781. 它们均

由 T.Forbs 于 1997 年发现的. 在此之前的记录是由 G.Löh 于 1989 年给出的，长度分别为 12(第一类) 和 13(第二类).

5.3 Wieferich 素数

满足同余式

$$2^{p-1} \equiv 1 \pmod{p^2}$$

的素数 p 应当叫作 Wieferich 素数，因为 Wieferich 在 1909 年证明了如下一个困难的定理：

如果费马猜想第一种情形对于素数 p 不成立，则必有上面的同余式.

同余式 $2^{p-1} \equiv 1 \pmod{p}$ 对每个奇素数 p 均成立，但是 Wieferich 同余式只对很少的素数 p 成立. 在计算机时代之前，Meissner 和 Beeger 分别于 1913 和 1922 年发现 $p = 1093$ 和 3511 满足 Wieferich 同余式. 如果你是喜欢动手的读者，一定会在第二章 2.3 节计算过 $2^{1092} \equiv 1 \pmod{1093^2}$. 不难验证 3511 有同样性质.

记录

Lehmer 在 1981 年证明了：在 6×10^9 以内只有素数 1093 和 3511 满足 Wieferich 同余式. Crandall, Dilcher 和 Pomerance(1977) 又把计算扩大到 4×10^{12}, 后来 R.McIntosh,R.Brown 和 J.K.Crump(及其合作者) 又分别把计算扩大到 $8 \times 10^{12}, 49 \times 10^{12}$ 和 2×10^{14}. 最近 J.Knauer 和 J.Richstein 运用互联网把计算扩大到 1.25×10^{15}(见他们 2003 年的短文), 均没有发现新的 Wieferich 素数.

根据第二章 2.3 、2.4 节引述的结果，以上的计算表明，每个

拟素数的素因子 $p^2(p < 1.25 \times 10^{15})$ 只可能为 $p = 1093$ 或 3511. 这由 Pinch(2000) 通过数值计算所肯定. 在 10^{13} 以内, 他检查出 54 个有重因子的拟素数.

1910 年, Mirimanoff 证明了与 Wieferich 定理相似的以下定理:

如果费马猜想第一种情形对素指数 p 不成立, 则 $3^{p-1} \equiv 1 \pmod{p^2}$.

可以验证 1093 和 3511 不满足 Mirimanoff 同余式.

这两个结果开创了攻击费马猜想第一种情形的新路线. 由于 Vandiver, Frobenius, Pollaczek, Morishima, Rosser 和近来 Granville 和 Monagan (1988), Suzuki (1994) 的工作, 费马猜想第一种情形对于更大范围都是对的. 在这方面, 一个重要的进展是 Gunderson 的组合方法将许多判别法合在一起. 这可参见我的书, 那里有完全的参考文献.

费马猜想已被完全证明, 上述的进展已成为历史. 但是上面提到的那些同余式在其他数论问题中仍是重要的.

更一般地, 对每个基 $a \geqslant 2$(a 可以为素数或者为合成数), 我们可以考虑满足 $p \nmid a$, $a^{p-1} \equiv 1 \pmod{p^2}$ 的素数 p. 阿贝尔最早 (1828 年) 问到是否有这样的例子. 而雅可比给出了例子, 对于 $p \leqslant 37$ 得到以下同余式:

$$3^{10} \equiv 1 \pmod{11^2}$$

$$9^{10} \equiv 1 \pmod{11^2}$$

$$14^{28} \equiv 1 \pmod{29^2}$$

$$18^{36} \equiv 1 \pmod{37^2}$$

商式

$$q_p(a) = \frac{a^{p-1} - 1}{p}$$

叫作 (以 a 为基)p 的费马商．费马商模 p 余数有类似于对数的性质 (爱森斯坦在 1850 年已经注意到这些性质)：若 $p \nmid ab$, 则

$$q_p(ab) \equiv q_p(a) + q_p(b) \pmod p$$

又有

$$q_p(p-1) \equiv 1 \pmod p, \qquad q_p(p+1) \equiv -1 \pmod p$$

我在 1983 年的文章 " 1093 " 中指出费马商的许多有趣的性质．举一个例子，下面的同余式是爱森斯坦于 1850 年发现的：

$$q_p(2) \equiv \frac{1}{p}\left(1 - \frac{1}{2} + \frac{1}{3} - \frac{1}{4} + \cdots - \frac{1}{p-1}\right) \pmod p$$

下列问题至今未解决：

(1) 给了 $a \geqslant 2$, 是否有无穷多素数 p, 使得 $a^{p-1} \equiv 1 (\bmod\ p^2)$?

(2) 给了 $a \geqslant 2$, 是否有无穷多素数 p, 使得 $a^{p-1} \not\equiv 1 (\bmod\ p^2)$?

问题 (1) 的答案应当是肯定的，但是这没有什么根据，而且这个问题显然是很困难的．下一个问题是固定素数但是基改变：

(3) 若 p 为奇素数，是否有一个或更多的 a, $2 \leqslant a < p$, 使得 $a^{p-1} \equiv 1 (\bmod\ p^2)$?

这方面有一些结果． Kruyswijk 在 1966 年证明了：存在常数 C, 使得对每个奇素数 p

$$\#\{a \mid 2 \leqslant a < p,\ a^{p-1} \equiv 1 (\bmod\ p^2)\} < p^{\frac{1}{2} + \frac{C}{\lg \lg p}}$$

所以对每个素数 p, 好的基 a 不太多．

1987 年 Granville 证明了

$$\#\{\text{素数 } q \mid 2 \leqslant q < p,\ q^{p-1} \equiv 1 (\bmod\ p^2)\} < p^{1/2}$$

更一般地，若 $u \geqslant 1$ 而 p 为素数，并且 $p \geqslant u^{2u}$, 则

$$\#\{\text{素数 } q \mid 2 \leqslant q \leqslant u^{1/u},\ q^{p-1} \equiv 1(\bmod p^2)\} \geqslant up^{u/2}$$
$$\#\{\text{素数 } q \mid 2 \leqslant q < p,\ q^{p-1} \not\equiv 1(\bmod p^2)\} \geqslant \pi(p) - p^{1/2}$$

2001 年，Keller 和 Richstein 对于 $p = 6692367337$ 决定出共 16 个基 a, $2 \leqslant a < p$, 使得 $a^{p-1} \equiv 1 \pmod{p^2}$, 它们是 $a = 5^k$ $(1 \leqslant k \leqslant 14)$,$a = 4961139411$ 和 $a = 6462265338$. 对于 $p = 188748146801$, 考查到有同样多的 $a < p$, 即 $a = 5^k$ $(1 \leqslant k \leqslant 16)$. 在此之前的记录由 Ernvall 和 Metsänkylä 于 1997 年给出：$p = 1645333507$ 有 14 个基 $a < p$. 上述三个 p 均满足 $5^{p-1} \equiv 1 \pmod{p^2}$. 请比较表 5.3.

Powell 证明了：若 $p \not\equiv 7 \pmod 8$, 则至少有一个素数 $q < \sqrt{p}$, 使得 $q^{p-1} \not\equiv 1 \pmod{p^2}$(此问题于 1982 年在《美国数学月刊》中提出，由 Tzanakis 于 1986 年发表解法). 利用更强的方法可证对每个素数 $p \geqslant 11$, 均存在素数 q, $2 \leqslant q < (\lg p)^2$, 使得 $q^{p-1} \not\equiv 1 \pmod{p^2}$.

Lehmer 对于以 2 为基的费马商作了计算, 这促使 Riesel(1964), Kloss(1965), Brillhart, Tonascia 和 Weinberger(1971) 公布了基一直到 100 的费马商表, 指数 p 不断地增大. 这些结果又被 Aaltonen 和 Inkeri(1991),Montgomery(1993),Keller 和 Richstein(2001) 不断扩大. 最后的表中素数基 $a < 1000$ 和素数指数 $p < 10^{11}$. 对于 $a = 3$ 和 5,p 一直算到 10^{13}. 表 5.3 是从中摘取的一部分, 素数基到 100, 标有 C, K, M 和 R 的解分别由 D.Clark,W.Keller,P.L.Montgomery 和 J.Richstein 发现的.

表 5.3　被 p 整除的费马商

基	满足 $a^{p-1} \equiv 1 \pmod{p^2}$ 的素数 p
2	1093　3511
3	11　1006003
5	20771　40487　53471161　1645333507^{M}　6692367337^{K}　188748146801^{K}
7	5　491531
11	71
13	863　1747591
17	3　46021　48947
19	3　7　13　43　137　63061489
23	13　2481757　13703077　15546404183^{R}
29	
31	7　79　6451　2806861^{K}
37	3　77867　76407520781^{R}
41	29　1025273　138200401^{K}
43	5　103
47	
53	3　47　59　97
59	2777
61	
67	7　47　268573
71	3　47　331
73	3
79	7　263　3037　1012573^{K}　60312841^{K}
83	4871　13691　315746063^{C}
89	3　13
97	7　2914393^{K}　76704103313^{R}

5.4　Wilson 素数

本节很短，因为事情知道的很少.

Wilson 定理是说：若 p 为素数，则 $(p-1)! \equiv -1 \pmod{p}$. 所

以 Wilson 商

$$W(p)=\frac{(p-1)!+1}{p}$$

是整数. 若 $W(p)\equiv 0\ (\mathrm{mod}\ p)$(即 $(p-1)!\equiv -1\ (\mathrm{mod}\ p^2)$), 称 p 为 Wilson 素数. 如 $p=5,13$ 为 Wilson 素数. 目前不知是否存在无穷多个 Wilson 素数. 关于此, Vandiver 写到:

这个问题似乎有这样一个特点: 假如我死而复活, 某位数学家告诉我这个问题已经完全解决, 我想我马上又会死去.

记录

除了 5 和 13 之外, 目前还只知道 563 是 Wilson 素数, 它是由 Goldberg 于 1963 年发现的, 是计算机搜索早期成功的例子之一. 后来 E.H.Pearson,K.E.Kloss,W.Keller,H.Dubner 一直寻找 Wilson 素数. 最后由 Gonter 和 Kundert 在 1988 年找到 10^7. 而 Crandall,Dilcher 和 Pomerance 于 1997 年找到 5×10^8, 都没有找到新的 Wilson 素数.

5.5 全 1 素数

十进制表成全 1 的数 $1,11,111,1111,\cdots$ 有奇妙的性质, 它们叫作全 1 数. 它们何时为素数?

我们用 Rn 表示连续 n 个 1 的数

$$111\cdots 1=\frac{10^n-1}{9}$$

若 Rn 为素数, 则 n 必为素数, 因为当 $n,m>1$ 时,

$$\frac{10^{nm}-1}{9}=\frac{10^{nm}-1}{10^m-1}\cdot\frac{10^m-1}{9}$$

而两个因子均大于 1.

记录

目前已知的全 1 素数只有 $R2, R19, R23$, 以及计算机时代的 $R317$ (Williams 于 1978 年发现) 和 $R1031$ (Williams 和 Dubner 于 1986 年发现). 另一方面, Dubner 于 1992 年验证了 $p < 20000$ 不再有其他全 1 素数 Rp. 计算工作由 J.Young,T.Granlund 和 H.Dubner 继续到 $p < 60000$.Dubner 于 1999 年 9 月发现 $R49081$ 可能是素数 (发表于 2002 年), 而 L.Baxter 等人于 2000 年 10 月发现 $R86453$ 可能是素数. 但是目前还没有希望判定这么大数的素性.

现在已经对所有 $p \leqslant 211$ 得到了全 1 数 Rp 的素因子分解式.

问题: 是否有无穷多个全 1 素数?

关于全 1 数的进一步结果可见 Yates(1982) 的书.

不难看出: 大于 1 的全 1 数不是完全平方数. 进一步可证它们也不是立方数 (见 Rotkiewitz 1987). 它们也不是 5 次方 (R.Bond 和 K.Inkeri 均于 1989 年写信告诉我). 当 k 不为 2, 3 或 5 的倍数时, 现在不知是否有 k 次方的全 1 数 (见 Obláth 1956).

1979 年, Williams 和 Seah 研究形如 $(a^n-1)/(a-1)$ 的数, 其中 $a \neq 10, 2$($a = 2$ 为 $2^n - 1$, 而 $a = 10$ 即为全 1 数). 这些数现在叫作 a 进制的全 1 数. 和通常全 1 数一样, 只有 n 为素数时它们才可能为素数. 这类数很大时, 判别它们是否为素数通常也是困难的.

在表 5.4 中, 括号内的数表示 n 已经计算的上界. Dubner 于 1993 年发表了如下范围的结果: 对于 $a = 3, 5, 6$, $n \leqslant 12000$; 对于 $a = 7$, $n \leqslant 10700$; 对于 $a = 11$, $n \leqslant 11000$; 对于 $a = 12$, $n \leqslant 10400$. 他的更大的表中包含所有 $a \leqslant 99$ 的情形. 目前最大的表是由 A.Steward 给出的.

表 5.4　形如 $(a^n-1)/(a-1)$ 的素数

a	n
3	3　7　13　71　103　541　1091　1367　1627　4177[DB]　9011*　9551*　36913*　[42700]
5	3　7　11　13　47　127　149　181　619　929　3407*　10949*　13241*　13873*　16519*　[31400]
6	2　3　7　29　71　127　271　509　1049　6389*　6883[S]　10613*　19889*　[29800]
7	5　13　131　149　1699[DB]　14221*　[28200]
11	17　19　73　139　907　1907*　2029*　4801[B]　5153*　10867*　20161*　[24000]
12	2　3　5　19　97　109　317　353　701　9739*　14951*　[26300]

表 5.4 中带有星号的可能为素数. 在表中已确定为素数的, 其最大者标以 DB, 表示由 H.Dubner 和 R.P. Brent(1996) 证明, 标以 B 的表示由 D.Broadhurst(2000) 证明, 标以 S 的表示由 A.Steward(2001) 证明.

5.6　数 $kb^n \pm 1$

我在第二章讲过，费马数的因子均有形式 $k2^n+1$. 这类数从而引起人们注意，人们自然会研究这些数的素性. 除了 Mersenne 数 $(k=1)$ 之外，其他形如 $k2^n-1$ 的数也被判定何时为素数.

根据狄利克雷关于算术级数中的素数定理，对给定的 $n \geqslant 1$, 存在无穷多整数 $k \geqslant 1$, 使得 $k2^n+1$ 为素数. 也有无穷多个整数 $k' \geqslant 1$, 使得 $k'2^n-1$ 为素数.

一个有趣的问题是: 当 k 固定时, 即给定 $k \geqslant 1$, 是否存在整数 $n \geqslant 1$, 使得 $k2^n+1$(或者 $k2^n-1$) 为素数？这个问题由 Bateman 提出. 而由 Erdös 和 Odlyzko 于 1979 年给出答案. 我引述他们的部分结果.

对每个实数 $x \geqslant 1$, 令

$$N(x) = \#\{\text{奇数}k \mid 1 \leqslant k \leqslant x, \text{存在}n \geqslant 1, \text{使}k2^n + 1\text{为素数}\}$$

则存在有效可计算的 $C_1 > 0$, 使得对每个 $x \geqslant 1$, $N(x) \geqslant C_1 x$. 将 $k2^n + 1$ 改成 $k2^n - 1$ 也有类似结果，并且所用的方法可研究其他类似的数列.

既使集合 $\{k \mid 1 \leqslant k \leqslant x, \text{有}n \geqslant 1\text{使 } k2^n + 1\text{为素数}\}$ 具有正的比例 (改用 $k2^n - 1$ 也如此), 但是 Riesel 在 1956 年发现了 $k = 509203$, 对于所有 $n \geqslant 1$, $k2^n - 1$ 都是合成数. 他的文章用瑞典文写的， Sierpiński 肯定不知道这篇文章. Sierpiński 在 1960 年证明了如下有趣的定理:

> *存在无穷多个奇数 k, 使得对每个 $n \geqslant 1, k2^n + 1$ 均是合成数.*

具有上述性质的 k 叫作 Sierpiński 数. 如果奇数 k 有性质：对每个 $n \geqslant 1$, $k2^n - 1$ 均为合成数，则 k 自然地叫作 Riesel 数.

由狄利克雷关于算术级数的素数定理和 Sierpiński 结果，可知有无穷多个 Sierpiński 数为素数. 类似地，有无穷多个 Riesel 数为素数.

记录

目前已知的最小 Sierpiński 数是 Selfridge 于 1963 年决定的 $k = 78557$. 目前已知的最小 Riesel 数是 Riesel 自己给出的 $k = 509203$.

Keller 多年来试图证明 $k = 78557$ 是最小的 Sierpiński 数. 他在 1991 年只证明了 $k \geqslant 4847$, 并且在 $4847 \leqslant k < 78557$ 当中只有 35 个奇数可能是 Sierpiński 数. 1997 年 J.Young 又从中删

掉了 14 个. 后来在 Gallot 方案的帮助下又删掉 4 个： 2 个由 M.Thibeault(1999) 删掉， 1 个由 L.Baxter(2001 年 4 月) 删掉，另 1 个由 J.Szmidt(2001 年 11 月) 删掉. 再后来 L.Helm 和 D.Norris 领导的一个分布式计算方案在几周之内又成功地删掉了 5 个，最后只剩下 12 个还需要进一步考查：

$$k = 4847, 5359, 10223, 19249, 21181, 22699,$$

$$24737, 27653, 28433, 33661, 55459, 67607$$

对于可能的 Riesel 数 $k < 509203$,Keller 证明了 $k \geqslant 659$. 在众多人参与寻找工作之下，还剩下 101 个数需要考查.

这种试图删掉可能 k 值的计算工作也导致发现大素数. 例如，消去 $k = 54767$ 作为可能的 Sierpiński 数，同时也发现了一个 402569 位的素数 (见表 5.5). 又如， O.Heaberlé(2003 年 3 月) 消去 $k = 204223$ 为可能的 Riesel 数，这也同时得到一个素数 $204223 \times 2^{696891} - 1$(共 209791 位), 而当 $n < 696891$ 时，$204223 \times 2^n - 1$ 均为合成数.

记录

目前已知形如 $k2^n + 1$ 的最大素数是 $3 \times 2^{2145353} + 1$(645817 位，见表 5.5), 它也是费马数目前已知的最大因子 (见第二章 2.6 节). 目前已知形如 $k2^n - 1$ 的最大素数是 J.Penné 和 P.Jobling 在 2003 年发现的 $138847 \times 2^{1283793} - 1$(386466 位).

目前所知 4 个最大的素数均为 Mersenne 数. 表 5.5 给出 Mersenne 素数之外最大素数的一个清单. 其中最前面两个素数超过一个 Mersenne 素数，是用 GIMPS 找到的.

广义费马数

上面素数中多数有形式 $b^{2^m}+1$, 即为 kb^n+1 的特殊情形 ($k=1, n=2^m, b$ 为偶数). 形如 $b^{2^m}+1(b\geqslant 2, m\geqslant 1)$ 的数叫作广义费马数. 1985 年, Dubner 首次列出这种形式的一些大素数 (叫作广义费马素数), 其中最大者为 $150^{2^{11}}+1$(4457 位).

Y.Gallot 约在 1998 年注意到: 试验广义费马数和同样大小的 Mersenne 数的素性所花时间差不多相同. 随后他建立并优化了一个计算机程序, 实现了他的看法. 实际试验中比 $k>1$ 的每个数 $k2^n\pm 1$ 都要快. 算法中使用了 Crandall 和 Fagin(1994) 的离散加权变换 (DWT), 这种变换也曾用于发现目前所知的五个最大的 Mersenne 素数.

表 5.5　目前已知的最大非 Mersenne 素数

素数	位数	发现人	年份
$3\times 2^{2145353}+1$	645817	J.Cosgrave, P.Jobling, G.Woltman and Y.Gallot	2003
$62722^{2^{17}}+1$	628808	M.Angel, P.Carmody and Y.Gallot	2003
$1483076^{2^{16}}+1$	404434	D.Heuer, J.Fougeron and Y.Gallot	2003
$1478036^{2^{16}}+1$	404337	D.Heuer, J.Fougeron and Y.Gallot	2002
$54767\times 2^{1337287}+1$	402569	P.Coels, L.Helm, D.Norris, G.Woltman and Y.Gallot	2002
$1361846^{2^{16}}+1$	402007	A.J.Penrose, J.Fougeron and Y.Gallot	2002
$1266062^{2^{16}}+1$	399931	D.Underbakke and Y.Gallot	2002
$5\times 2^{1320487}+1$	397507	M.Toplic and Y.Gallot	2002

历史上所知的最大素数几乎都是 Mersenne 素数. 直到 1989 年 8 月, 六位数字专家 J. Brown, L. C. Noll, B. Parady, G. Smith, J. Smith 和 S. Zarantonello 发现了素数 $391581\times 2^{216193}-1$, 把

Mersenne 素数 M_{216091} 甩在后边. 可怜的 Mersenne, 他曾满怀忧虑和悲伤地在他的墓前绕来绕去. 由于他的 Mersenne 素数杰出的表现，他又可以安息了. 但是他的安静能持续多久？

Dubner 和 Gallot(2002) 在他们最近一篇文章中认为存在很多大的广义费马素数. 用他们的话说，适当组织的寻找工作不久会改变已知最大素数的现况. 已经决定出 100000 位以上的大约 120 个这种形式的素数.

对于形如 $k \cdot b^n + 1$ $(b > 2)$ 数的其他记录还有:

记录

(1) 表 5.5 中的素数 $62722^{2^{17}} + 1$ 是形如 $N^2 + 1$ 的已知最大素数. 我们不知这种形式的素数是否有无穷多个.

(2) 形如 $k \cdot b^n + 1$ $(k > 1, 2 \nmid b)$ 的已知最大素数为 G.Löh 和 Y.Gallot 于 2002 年发现的 $82960 \times 31^{82960} + 1$(123729 位).

Cullen 数

形如 $Cn = n \cdot 2^n + 1$ 的数叫 Cullen 数. Robinson 于 1958 年证明了 $C141$ 是素数，而对 $1 < n \leqslant 1000$ 的所有其他的 n,Cn 都是合成数. 在 25 年里，除了 $C1 = 3$ 之外这是唯一知道的 Cullen 素数. 在 1987 年 (发表于 1995 年),Keller 决定出 $n \leqslant 30000$ 的所有素数 Cn, 后来用 Y.Gallot 的算法又发现更多. 表 5.6 所列相信是 $n \leqslant 633000$ 的全部 Cullen 素数.

Hooley 在书 (1976) 中指出，几乎所有的 Cullen 数都是合成数，即

$$\lim_{x \to \infty} \frac{C\pi(x)}{x} = 0$$

其中 $C\pi(x)$ 表示 x 以内 Cullen 素数 Cn 的个数. 但是我们不知道是否存在无穷多个 Cullen 素数 Cn.

数 $Wn = n \cdot 2^n - 1$ 叫作 Woodall 数，也叫第二类 Cullen 数.

表 5.6　Cullen 素数 Cn

n	发现人	年份
481899	M.Morii and Y.Gallot	1998
361275	D.Smith and Y.Gallot	1998
262419	D.Smith and Y.Gallot	1998
90825	J.Young	1997
59656	J.Young	1997
32469	M.Morii	1997
32292	M.Morii	1997
18496	W.Keller	1984
6611	W.Keller	1984
5795	W.Keller	1984
4713	W.Keller	1984
141	R.M.Robinson	1958
1	—	—

对于 $n \leqslant 20000$, Wn 为素数的情形只有 $n = 2, 3, 6, 30, 75, 81$ (Riesel　1969),115, 123, 249, 362, 384, 462, 512, 751, 822, 5312, 7755, 9531, 12379, 15822 和 18885(Keller　1987). 后来 J.Young 算到 $n \leqslant 100000$,Y.Gallot 及其合作者算到 $n \leqslant 416000$. 表 5.7 给出 $n > 20000$ 情形的已知 Woodall 素数.

表 5.7　已知最大的 Woodall 素数 Wn

n	发现人	年份
667071	M.Toplic and Y.Gallot	2000
151023	K.O'Hara and Y.Gallot	1998
143018	R.Ballinger and Y.Gallot	1998
98726	J.Young	1997
23005	J.Young	1997
22971	J.Young	1997

W.Keller 和 W.Niebuhr(1995) 对于所有 $n \leqslant 300$ 的数 Cn 和

Wn 给出完全分解式. 这种分解又由 P.Leyland 扩大到所有 $n \leqslant 400$(1998 年 11 月) 和所有 $n \leqslant 450$(2000 年 8 月). 在其他人的帮助下, 近来又扩大到所有 $n \leqslant 500$(2002 年 1 月).

两类 Cullen 数可推广成 $n \cdot b^n + 1$ 和 $n \cdot b^n - 1(b > 2)$.Dubner 于 1989 年引进广义 Cullen 数 $n \cdot b^n + 1$, 研究它们为素数的情况, 发现当 b 是大于 3 的素数时, 几乎不存在素数 $n \cdot b^n + 1$. 但是对每个素数 $b > 2$ 似乎都没有证明形如 $n \cdot b^n + 1$ 的素数是不存在的. 事实上, 对于 $b = 13, 17, 19, 23, 29, 31, 41, 47, 53, 71, 73$, 均没有发现形如 $n \cdot b^n + 1$ 的素数. 但是对这些 b 也没能证明这种素数是不存在的.

大量计算表明: 对给定的 b, $n \cdot b^n + 1$ 为素数时, 其 n 均很大. 利用 Gallot 算法于这个问题, 对于 $b = 19, 23$(Keller 和 Gallot 1998) 和 $b = 17, 71$(Löh 和 Gallot 2000) 终于发现了形如 $n \cdot b^n + 1$ 的"最小" 素数. 最近 Löh 对于 $b = 31$ 发现了素数 $82960 \times 31^{82960} + 1$. 我们在前面已提到过它.

5.7 素数和二阶线性递归序列

在 5.1 节中曾考虑过由二阶线性递归方式定义的序列 $T = (T_n)_{n \geqslant 0}$.

广义二阶线性递归序列

设 P, Q 为给定的非零整数, 并且 $D = P^2 - 4Q \neq 0$.P 和 Q 是下面定义的序列 $T = (T_n)_{n \geqslant 0}$ 的参数. 设 T_0, T_1 为整数 (不同时为 0), 对每个 $n \geqslant 2$, 令

$$T_n = PT_{n-1} - QT_{n-2}$$

序列 T 的特征多项式为 $X^2 - PX + Q$, 它的根为

$$\alpha = \frac{P + \sqrt{D}}{2}, \qquad \beta = \frac{P - \sqrt{D}}{2}$$

于是 $\alpha + \beta = P, \alpha\beta = Q, \alpha - \beta = \sqrt{D}$.

对于参数 (P, Q) 的两个序列 $(U_n)_{n\geqslant 0}$ 和 $(V_n)_{n\geqslant 0}$, 其中 $U_0 = 0, U_1 = 1, V_0 = 2, V_1 = P$, 它们即是第二章 2.4 节已经考虑过的 Lucas 序列.

令 $\gamma = T_1 - T_0\beta, \delta = T_1 - T_0\alpha$, 则不难证明对每个 $n \geqslant 0$

$$T_n = \frac{\gamma\alpha^n - \delta\beta^n}{\alpha - \beta} = T_1\frac{\alpha^n - \beta^n}{\alpha - \beta} + QT_0\frac{\alpha^{n-1} - \beta^{n-1}}{\alpha - \beta}$$

若 $U = (U_n)_{n\geqslant 0}$ 是与 T 有同样参数的 Lucas 序列, 则 $T_n = T_1U_n - QT_0U_{n-1} (n \geqslant 2)$.

还可以定义如下的伴随序列 $W = (W_n)_{n\geqslant 0}$, 其中

$$W_0 = 2T_1 - PT_0, \qquad W_1 = T_1P - 2QT_0$$

$$W_n = PW_{n-1} - QW_{n-2} \ (n \geqslant 2)$$

则 $W_n = \gamma\alpha^n + \delta\beta^n = T_1V_n - QT_0V_{n-1}$, 其中 $V = (V_n)_{n\geqslant 0}$ 是伴随的 Lucas 序列, 具有参数 (P, Q).

像第二章 2.4 节讲述 Lucas 序列一样, 一般序列也有许多代数关系和整除性质. 但我的目标是只研究与素数有关的性质.

序列 T的素因子

考虑集合

$$\mathcal{P}(T) = \{\text{素数 } p \mid \text{存在 } n \geqslant 0 \text{使得 } T_n \neq 0 \text{但是 } p \mid T_n\}$$

若 $\alpha/\beta = \eta$ 是单位根, 称序列 T 是退化的. 这时 $\beta/\alpha = \eta^{-1}$

也是单位根，从而 $|\eta+\eta^{-1}|\leqslant 2$. 但是

$$\eta+\eta^{-1}=\frac{\alpha^2+\beta^2}{\alpha\beta}=\frac{P^2-2Q}{Q}$$

所以若 T 是退化的，则 $P^2-2Q=0,\pm Q$ 或 $\pm 2Q$.

不难证明：若 T 是退化的，则 $\mathcal{P}(T)$ 是有限集合. 1954 年 Ward 证明逆命题成立

对任何非退化的序列 T,$\mathcal{P}(T)$ 是无限集合.

一个自然的问题是：$\mathcal{P}(T)$ 是否一定有正密度？能否计算这个密度？

Hasse(1966) 做了开创性工作，他的目标是研究使得 2 模 p 的阶为偶数的素数 p 所组成的集合. 这条件相当于存在 $n\geqslant 1$, 使得 $p\mid 2^{2n}-1$ 但是对所有 $1\leqslant m<2n$,$p\nmid 2^m-1$. 于是 $2^n\equiv -1 \pmod p$, 即 $p\mid 2^n+1$. 反之，若 $p\mid 2^n+1$, 则 2 模 p 的阶为偶数 $2n$.

序列 $H=(H_n)_{n\geqslant 0}$，$H_n=2^n+1$ 是参数 $(P,Q)=(3,2)$ 的伴随 Lucas 序列. 对于 $x\geqslant 0$ 令

$$\pi_H(x)=\#\{p\in\mathcal{P}(H)\mid p\leqslant x\}$$

Hasse 证明了

$$\lim_{x\to\infty}\frac{\pi_H(x)}{\pi(x)}=\frac{17}{24}$$

数 $\frac{17}{24}$ 表示除尽 H 的素数 p(即指 p 除尽某个 H_n) 的密度. 1985 年，Lagarias 又用 Hasse 方法证明了对 Lucas 数列 $V=(V_n)_{n\geqslant 0}$,$\mathcal{P}(V)$ 的密度为 2/3.

人们倾向于猜想：对每个非退化的序列 T, 集合 $\mathcal{P}(T)$ 均有正密度.

序列 T 中的素数项

现在讲另一个有趣而困难的问题. 设 $T = (T_n)_{n\geqslant 0}$ 是二阶线性递归序列, 如 Fibonacci 数列或 Lucas 数列, 它们都包括素数, 但不知并且很难决定是否包含无穷多个素数.

由第二章 2.4 节的关系 (4.15) 和 (4.16) 可知:

若 U_m 为素数, 则 $m = 4$ 或者 m 为素数;

若 V_m 为素数, 则 $m = 2^t$ 或者 m 为素数.

当然反过来都不正确.

有许多计算工作致力于寻求 Fibonacci 素数和 Lucas 素数, 以及这些数的因子分解 (见第二章 2.11D 节). 由于这些数列增长很快, 这些数的分解和素性判定都很困难.

这方面发表的工作有 Jarden 1958 年的书, Brillhart 于 1973 年改写和扩充成第三版. 文章有 Brillhart, Montgomery 和 Silverman(1988), Dubner 和 Keller(1999). 目前所知的结果如下:

对于 $n < 360000$,Fibonacci 数 U_n 为素数 (或可能为素数) 的有

$$\begin{aligned} n = {} & 3,4,5,7,11,13,17,23,29,43,47,83,131,137,359,431,433 \\ & 449,509,569,571,2971^{\mathrm{W}},4723^{\mathrm{WM}},5387^{\mathrm{WM}},9311^{\mathrm{DK}},9677^{\mathrm{deW}} \\ & 14431^{\mathrm{BdeW}},25561^{\mathrm{BdeW}},30757^{\mathrm{BdeW}},35999^{\mathrm{BdeW}},37511^{*},50833^{*} \\ & 81839^{\mathrm{BdeW}},104911^{*},130021^{*},148091^{*},201107^{*} \end{aligned}$$

某些数上的字母表示这些 Fibonacci 数的素性是由 H.C.Williams (W), H.C.Williams 和 F.Morain (WM), H.Dubner 和 W.Keller(DK), B. de Water(deW) 或者由 D.Broadhurst 和 B.de Water(BdeW) 所决定的. 指数 n 上有星号者表示只知它可能为素数, 即 U_n 通过一系列试验也没有试出它为合成数. 可能的素数 U_{37511} 和 U_{50833} 是 Dubner 发现的, 而后 4 个可能的素数依次由 de Water,D.Fox,

T.D.Noe 和 H.Lifchitz 所发现. 素数 U_{81839} 有 17103 位. 证明它是素数是一个值得注意的成绩.

对于 $n < 260000$,Lucas 数 V_n 为素数 (或可能为素数) 的有

$$
\begin{aligned}
n = {} & 2,4,5,7,8,11,13,16,17,19,31,37,41,47,53,61,71,79,\\
& 113,313,353,503^{\mathrm{W}},613^{\mathrm{W}},617^{\mathrm{W}},863^{\mathrm{W}},1097^{\mathrm{DK}},1361^{\mathrm{DK}},\\
& 4787^{\mathrm{DK}},4793^{\mathrm{DK}},5851^{\mathrm{DK}},7741^{\mathrm{DK}},8467^{\mathrm{deW}},10691^{\mathrm{DK}},\\
& 12251^{\mathrm{BdeW}},13963^{\mathrm{Oak}},14449^{\mathrm{DK}},19469^{\mathrm{BdeW}},35449^{\mathrm{deW}},\\
& 36779^{*},44507^{*},51169^{\mathrm{BdeW}},56003^{*},81671^{*},89849^{*},94823^{*},\\
& 140057^{*},148091^{*},159521^{*},183089^{*},193201^{*},202667^{*}
\end{aligned}
$$

其中记号与前有相同的意义, 只是加上一个证明素性的 M.Oakes (Oak). 其中可能的素数 $V_{36779}, V_{44507}, V_{81671}, V_{89849}$ 由 Dubner 发现, V_{140057}, V_{148091} 由 de Water 发现, 而 V_{94823} 和最后四个可能的 Lucas 素数由 H.Lifchitz 发现.

如果你再看一下这两个清单, 会发现当 $n = 5,7,11,13,17$ 和 47 时, U_n 和 V_n 均为素数. 再继续看下去, 则一直到 $n = 148091$,U_n 和 V_n 才同时可能为素数. 如果能证这两个数确实为素数, 我们也许会感到存在无穷多个 n, 使得 U_n 和 V_n 同时为素数. 这个问题 "坚如硬壳". 核桃壳很难消化, 不要影响您晚上的睡眠.

只由合成数组成的序列 T

如果 T 不是 Lucas 序列或伴随 Lucas 序列, 则 T 可以不含任何素数. Graham 在 1964 年发现第一个例子, 其中 $P = 1, Q = -1$, 但是在计算 T_0 和 T_1 时有错. 后来 Knuth 于 1990 年给出正确值

$$T_0 = 331635635998274737472200656430763$$

$$T_1 = 1510028911088401971189590305498785$$

还给出一个较小的例子

$$T_0 = 62638280004239857$$

$$T_1 = 49463435743205655$$

对于 $P=3, Q=2$,Lucas 和伴随 Lucas 序列为 $U_n = 2^n - 1$ 和 $V_n = 2^n + 1$, 这些序列均包含素数. 仍对于 $P=3, Q=2$, 但是取 $T_0 = k+1, T_1 = 2k+1$, 则得到序列 $T_n = k \cdot 2^n + 1$. 如果 $T_0' = k-1, T_1' = 2k-1$, 则给出 $T_n' = k \cdot 2^n - 1$. 这些序列在前节已讨论过，已经说过：存在无穷多个奇数 k(Sierpiński 数), 使得 T_n 为合成数. 也存在无穷多个整数 k(Riesel 数), 使得 T_n' 为合成数.

2002 年， Izotov 给出无穷多对 (P, Q), 对于每对 (P, Q) 均有以它为参数的无穷多个序列 (具有不同的初始项) 均是由合成数组成.

NSW 数

NSW 不是“北南西” (North-South-West), 也不是“新南威尔士” (New South Wales), 而是指 Newman, Shanks 和 Williams 1980 年文章. 我有幸见到此文的预印本，我是在 Dan Shanks 访问 Queen 大学时见到此文，这次访问有许多理由是值得记忆的.

在文章中这些 NSW 数定义成奇数下标：$S_1 = 1, S_3 = 7, S_5 = 41, S_7 = 239, S_9 = 1393, \cdots$ 来源于如下的问题：是否存在阶为平方数的有限单群？

数 $W_n = S_{2n+1} (n \geqslant 0)$ 是以 $P=6, Q=1$ 为参数，初始项为 $W_0 = 1, W_1 = 7$ 的 2 阶线性递归序列. 从而对每个 $n \geqslant 2$

$$W_n = \frac{(1+\sqrt{2})^{2n+1} + (1-\sqrt{2})^{2n+1}}{2}$$

目前不知道是否有无穷多个 NSW 素数. 另一方面， Sellers

和WIlliams (2002) 证明了序列 $(W_n)_{n\geqslant 0}$(和许多类似序列) 中包含无穷多个合成数.

用原来的记号：如果 S_{2n+1} 是素数，则 $2n+1$ 必为素数．在 $p<2000$ 时，只有以下情形 S_p 为素数：

$$p=3,5,7,19,29,47,59,163,257,421,937,947,1493,1901$$

F.Morain 在 1989 年证明了 S_{1497} 和 S_{1901} 为素数． H.Dubner 在 1999 年对于区间 $2000<p<80000$ 决定出只有

$$p=6689,8087,9679,28953,79043$$

时， S_p 为可能的素数 (PRP), 此外在这个区间中没有其他素数．也在 1999 年， Dubner 和 Keller 证明了 S_{6689} 是素数．由于这些结果均未发表， W.Roonguthai 于 2000 年又重新独立发现前三个 PRP, 第四个又由 A.Walker 于 2001 年发现． D.Broadhurst 在 2001 年证明了 S_{8087}, S_{9679}(以及 S_{6689}) 是素数，证明很困难.



第六章　关于素数的经验和概率结果

"经验" (heuristic) 意味着根据试验. 经验结果是由对表中或扩大计算的数据加以观察而得到的. 有时, 这些结果表达了某种统计学分析的结论.

还有一种是概率方法. 我们在第四章引用过的 Cramér 文章 (1937), 对此有很好的解释:

> 在研究算术函数的渐近性质时, 常常能使用概率推理. 例如我们研究一个给定整数集合 S 的分布, 便把 S 看成是无穷多序列类 C 中一个成员. 它可具体解释成某种随机博弈的可能实现. 然后在许多情形下, 可以用概率等于 1 的方式证明在 C 中有某个关系 R, 即在确定的数学意义下, C 中几乎所有的序列均满足关系 R. 当然, 我们一般地不能保证 R 被这个特别序列 S 所满足, 但是用此法建议的结果随后常常会被人用其他严格的方法所证明.

如果使用经验方法或概率方法不够谨慎和缺乏智慧, 可能会得到与现实相距甚远的"梦想"式的数学. 应当避免过分草率的猜想和对数据的错误解读.

我仔细地限制自己, 只介绍少数可靠的贡献. 它们是 Hardy 和 Littlewood 在《数的分拆》(*PartitioNumerorum*) 中的一系列猜想, 和 Dickson,Bouniakowsky,Schinzel 和 Sierpiński 的一些诱人的猜想.

6.1 线性多项式的素数取值

我们又从狄利克雷算术级数素数定理开始，它是说：若 a 和 b 是整数，$a \neq 0, b \geqslant 1$ 并且 $\gcd(a, b) = 1$，则对于函数 $f(X) = bX+a$，存在无穷多个整数 $m \geqslant 0$，使得 $f(m)$ 为素数.

1904 年， Dickson 叙述了关于多个线性函数同时取值的如下的猜想：

(D) 设 $s \geqslant 1$，$f_i(X) = b_iX + a_i$，其中 a_i, b_i 为整数， $b_i \geqslant 1 (1 \leqslant i \leqslant s)$. 并设下面条件成立：

(∗) 不存在整数 $n \geqslant 1$，使得对每个整数 k 均有 $n \mid f_1(k)f_2(k)\cdots f_s(k)$.

则存在无穷多个自然数 m，使得 $f_1(m), f_2(m), \cdots, f_s(m)$ 均为素数.

下列命题比 (D) 要弱：

(D_0) 在对 $f_1(X), \cdots, f_s(X)$ 同样的假设下，存在某个自然数 m，使得 $f_1(m), f_2(m), \cdots, f_s(m)$ 均为素数.

初看一下，可能会怀疑 (D) 的正确性，而 (D_0) 似乎比 (D) 要求的要少很多，所以 (D_0) 更可接受. 但事实上 (D) 和 (D_0) 是等价的.

这是由于若 (D_0) 正确，则存在 $m_1 \geqslant 0$，使得 $f_1(m_1), \cdots, f_s(m_1)$ 均为素数. 令 $g_i(X) = f_i(X+1+m_1)$ $(1 \leqslant i \leqslant s)$，则 $g_1(X), \cdots, g_s(X)$ 也满足条件 (∗). 再由 (D_0) 知存在 $k_1 \geqslant 0$，使得 $g_1(k_1), \cdots, g_s(k_1)$ 均为素数. 令 $m_2 = k_1 + 1 + m_1 > m_1$，则 $f_1(m_2), \cdots, f_s(m_2)$ 均为素数. 继续下去便由 (D_0) 推出 (D).

Dickson 没有探索他的猜想的推论. 这是 Schinzel 和 Sierpiński

(1958) 文章的目标. 我对此文相当有兴趣, 在本章将用较大篇幅加以介绍.

Schinzel 实际上建议了一个更为广泛的猜想 (猜想 (H)), 其中多项式不必是线性的. 但是在我讨论猜想 (H) 和它的推论之前, 我先介绍 Schinzel 和 Sierpiński 在猜想 (D) 之下证明的许多有趣结果.

猜想 (D) 的一些重要推论列举如下, 这些推论表明猜想 (D) 即使成立, 要证明它也是十分遥远的.

(D_1) 设 $s \geqslant 1, a_1 < a_2 < \cdots < a_s$ 是非零整数序列, 并设 $f_1(X) = X + a_1, \cdots, f_s(X) = X + a_s$ 满足条件 (D) 中条件 $(*)$. 则存在无穷多整数 $m \geqslant 1$, 使得 $m + a_1, m + a_2, \cdots, m + a_s$ 为相邻素数.

在第四章 4.2 和 4.3 节讨论过的 Polignac(1849) 猜想是 (D_1) 的推论:

(D_2) 对每个偶数 $2k \geqslant 2$, 均存在无穷多对相邻素数, 每对素数都相差 $2k$. 特别地, 存在无穷多孪生素数对.

下面是关于孪生素数丰富性的另一个有趣的推论:

(D_3) 对每个整数 $m \geqslant 1$, 均存在 $2m$ 个相邻素数, 它们是 m 个孪生素数对.

下面是关于算术级数中素数的另一个相当意外的推论. 在第四章 4.4 节证明了: 若 $a, a + d, \cdots, a + (n - 1)d$ 均为素数, 而 $1 < n < a$, 则 d 为 $\prod_{p \leqslant n} p$ 的倍数. 由 (D_1) 可给出:

(D_4) 设 $n > 1, d$ 为 $\prod_{p \leqslant n} p$ 的倍数. 则存在无穷多个公差为 d 的算术级数, 其中每个算术级数均包含 n 个相邻素数.

请读者将这个非常强的猜想和我们在第四章 4.4 节中介绍的不依赖任何猜想的结果加以比较.

关于 Sophie Germain 素数，由 (D) 可以推出：

(D_5) *对每个 $m \geqslant 1$, 存在无穷多个算术级数，其中每个级数都是由 m 个 Sophie Germain 素数组成的.*

特别地, 由 (D) 推出存在无穷多个 Sophie Germain 素数, 而这个命题不用任何猜想从未被证明过. 我将在后面谈到关于 Sophie Germain 素数的分布的定量的命题.

猜想 (D) 是这样强的命题，它还可以推出：

(D_6) *存在无穷多个 Mersenne 数为合成数.*

我在第二章 2.4 节讲过，没有人 (不假设 (D)) 成功地证明了 (D_6). 但是容易对类似于 Mersenne 数的其他序列，可证明它包含无穷多个合成数. 下面结果是 Powell 于 1982 年提出的一个问题 (以色列人在 1983 年给出解答)：

若 m 和 n 为整数，$m > 1, mn > 2$(这就排除了 $m = 2, n = 1$), 则有无穷多个合成数 $m^p - n$, 其中 p 为素数

证明 设 q 为素数， $q \mid mn - 1$, 于是 $q \nmid m$. 若 p 为素数, $p \equiv q - 2 \pmod{q-1}$, 则 $m(m^p - n) \equiv m(m^{q-2} - n) \equiv 1 - mn \equiv 0 \pmod q$, 即 $q \mid m^p - n$. 由狄利克雷算术级数中的素数定理，存在无穷多素数 p 使得 $p \equiv q - 2 \pmod{q-1}$, 所以有无穷多个合成数 $m^p - n$, 其中 p 为素数. □

下面推论也可看出猜想 (D) 是很强的：

(D_7) *存在无穷多个 Carmichael 数，每个均为三个不同素数的乘积.*

Alford,Granvill 和 Pomerance(1994) 不用猜想 (D) 证明存在无穷多个 Carmichael 数，但是没有证明存在无穷多个 Carmichael 数，每个均恰好为三个素数的乘积.

(D) 的另一个重要的推论是著名的 Artin 猜想：

(A) 若 a 是非零整数，$a \neq -1$ 并且不是完全平方，则存在无穷多个素数 p, 使得 a 为模 p 的原根.

虽然 Artin 猜想至今未被证明，但是已有很重大的进展．首先， Gupta 和 Ram Murty(1984) 作出突破性工作，后来有 Heath-Brown(1986) 的摘取桂冠的工作，他证明了：至多有两个素数和三个无平方因子正整数， Artin 猜想对它不正确．

6.2 任意次多项式的素数取值

现在设多项式可以是非线性的．历史上第一个猜想是 1857 年由 Bouniakowsky 给出的，其中多项式次数至少为 2 ：

(B) 设 $f(X)$ 是整系数不可约多项式，次数 $\geqslant 2$ 并且首项系数为正．又设下列条件成立：

$(*)$ 不存在整数 $n>1$, 使得对每个整数 k,n 整除每个 $f(k)$. 则存在无穷多个自然数 m, 使得 $f(m)$ 均为素数.

就像猜想 (D) 和 (D_0) 等价一样，读者应当给出类似的猜想 (B_0), 并且猜想 (B) 和 (B_0) 等价．

在讨论猜想 (B) 之前，首先要明确，在多项式取素值方面目前只有很少的结果．例如，现在没有找到一个次数大于 1 的多项式 $f(X)$, 使得对无穷多自然数 n, $|f(n)|$ 均为素数．另一方面，Sierpiński 于 1964 年证明了：对每个 $k \geqslant 1$, 均存在整数 b, 使得对至少 k 个自然数 n,n^2+b 均为素数．

设 $f(X)$ 为次数 $d \geqslant 2$ 的整系数多项式．对每个 $x \geqslant 1$, 令

$$\pi_{f(X)}(x) = \#\{n \geqslant 1 \mid |f(n)| \leqslant x, \text{并且}|f(n)|\text{为素数}\}$$

Nagell 于 1922 年证明了 $\lim\limits_{x\to\infty} \pi_{f(X)}(x)/x = 0$, 所以 $f(X)$ 取很少的素值. Heilbronn 在 1931 年证明了更精细的结果:

存在正的常数 C(依赖于 $f(X)$), 使得对每个 $x \geqslant 1$

$$\pi_{f(X)}(x) \leqslant C\frac{x^{1/d}}{\lg x}$$

对于一般多项式, 目前知道的不多. 但是对某些特殊类型的多项式有较多的计算结果和猜想. 我以后再详细介绍.

是否存在无穷多个素数 p, 使得 $f(p)$ 均为素数, 这是更困难的问题. 特别地, 我已经讲过, 目前不知是否有无穷多个素数 p, 使得 $f(X) = X + 2$(或 $f(X) = 2X + 1$) 仍取素数值 (即不知无穷多孪生素数对或无穷多 Sophie Germain 素数的存在性). 但是如果考虑殆素数, 则用筛法并参见 Halberstam 和 Richert 的书, 可知情况要好得多.

回忆"殆素数"的定义: 给了 $k \geqslant 1$, 不超过 k 个素数 (不必不同) 之积的自然数 $n = p_1p_2\cdots p_r$ $(r \leqslant k)$ 叫作 k- 殆素数. 以 P_k 表示所有 k- 殆素数组成的集合. Richert(1969) 证明了:

设 $f(X)$ 是 $d \geqslant 1$ 次整系数多项式, 并且首项系数为正 $(f(X) \neq X)$. 又设对每个素数 p, $f(X) \equiv 0 \pmod p$ 的解数 $\rho(p)$ 小于 p. 再设当 $p \leqslant d+1$ 并且 $p \nmid f(0)$ 时, $\rho(p) < p - 1$. 则存在无穷多个素数 p, 使得 $f(p)$ 均为 $(2d+1)$- 殆素数.

Rieger(1969) 证明了下述特殊情形: 存在无穷多个素数 p, 使得 $p^2 - 2 \in P_5$.

现在回到 Bouniakowsky 猜想! Bouniakowsky 本人没有研究他的猜想的任何推论. 这是由 Schinzel 和 Sierpiński 做的. 他们在

100 年之后，独立地叙述了一个更一般的猜想.

下列命题未被证明，但它是猜想 (B) 的直接推论.

(B_1) 设 a, b, c 是两两互素的整数， $a \geqslant 1, a+b$ 和 c 不同时为偶数，如果 b^2-4ac 不为平方数，则存在无穷多个自然数 m，使得 am^2+bm+c 为素数.

命题 (B_1) 又推出：

(B_2) 若 k 为整数，并且 $-k$ 不是平方数，则存在无穷多个自然数 m，使得 m^2+k 为素数.

特别地，由 (B_2) 可知存在无穷多个形如 m^2+1 的素数. m^2+1 型素数和实二次域的类数有深刻的联系.

多项式 X^2+1 是判别式为负的最简单二次多项式. 如果能证明它可取无穷多个素数值，那将是一个巨大的进展. 但是只要与 Friedlander 和 Iwaniec(1998) 最近得到的下面重要定理相比，便知这是多么困难.

存在无穷多个素数可表成 a^2+b^4.

这个结果的证明需要深刻的筛法和其他工具. 这个结果离“形如 m^2+1 的素数有无穷多”还有多远？后者不仅包含 Friedlander 和 Iwaniec 定理，而且还推出对每个 $k \geqslant 1$，存在形如 $a^2+b^{2^k}$ 的无穷多素数.

下面的命题也是 Hardy 和 Littlewood 于 1923 年提出的猜想，它也是 (B) 的推论.

(B_3) 设 $d>1$ 为奇数，k 为整数，并且对 d 的每个因子 $e>1, k$ 都不是整数的 e 次幂. 则存在无穷多自然数 m，使得 m^d+k 为素数.

Schinzel 在与 Sierpiński 合写的文章中提出以下的猜想：

(H) 设 $s \geqslant 1$, $f_1(X), \cdots, f_s(X)$ 均是整系数不可约多项式，并且首项系数均为正整数. 又设下列条件成立：

(*) 不存在整数 $n > 1$, 使得对每个整数 k, $n \mid f_1(k)f_2(k)\cdots f_s(k)$. 则存在无穷多个自然数 m, 使得 $f_1(m), f_2(m), \cdots, f_s(m)$ 均为素数.

(H_0) 在对 $f_1(X), \cdots, f_s(X)$ 的同样假设之下, 存在自然数 m, 使得 $f_1(m), f_2(m), \cdots, f_s(m)$ 均为素数.

与前一样, (H) 和 (H_0) 是等价的. 如果 $f_1(X), \cdots, f_s(X)$ 都是一次多项式, 这就是 Dickson 的猜想 (D) 和 (D_0). 若 $s = 1$, 则为 Bouniakowsky 猜想 (B) 和 (B_0).

我不想列举这个猜想的所有推论, 但是想提一下 Schinzel 的一个结果, 它与 Carmichael 关于欧拉函数取值的一个猜想有联系. 回忆一下第二章 2.2F 节的记号. 对每个 $m \geqslant 1$, 令

$$V_\varphi(m) = \#\{n \geqslant 1 \mid \varphi(n) = m\}$$

Schinzel 在 1961 年证明由猜想 (H) 可推出:

(H_1) 对每个 $s > 1$, 存在无穷多整数 $m > 1$, 使得 $V_\varphi(m) = s$.

注意 $s \neq 1$, 所以命题 (H_1) 不包含 Carmichael 猜想.

喜欢毕达哥拉斯三角形的读者会知道, 有许多这样的三数组 (a, b, c), 其中 b 为偶数, $a^2 + b^2 = c^2$, 而 a 和 c 是素数, 如 $(3, 4, 5), (5, 12, 13)$ 等. 你可能会问是否有无穷多这样的三数组. 你可能想证明它, 但会遇到困难. 事实上, 没有人知道如何证明它. 除非假定猜想 (H) 是对的.

这是 Schinzel 和 Sierpiński 文章中所说的. 为了读者的方便, 我给出他们的证明. 首先需要建立:

(H_2) 设 a, b, c, d 为整数, $a > 0$, $d > 0$ 并且 $b^2 - 4ac$ 不是平方数. 又设存在整数 x_0, y_0, 使得 $\gcd(x_0 y_0, 6ad) = 1$ 并且 $ax_0^2 + bx_0 + c = dy_0$. 则存在无穷多对素数 p, q, 使得 $ap^2 + bp + c = dq$.

证明 $(H) \Rightarrow (H_2)$. 令 $f_1(X) = dX + x_0$, $f_2(X) = adX^2 +$

$(2ax_0+b)X+y_0$. 由于 $(2ax_0+b)^2-4ady_0=(2ax_0+b)^2-4a(ax_0^2+bx_0+c)=b^2-4ac$ 不是平方数, 可知 $f_2(X)$ 和 $f_1(X)$ 均是不可约的.

现在验证条件 (*). 记 $g(X)=f_1(X)f_2(X)$, 这是三次多项式, 首项系数为 ad^2. 如果存在素数 p, 使得对每个整数 m, 均有 $p\mid g(m)$, 则 p 整除 $g(m)-g(m-1)=\Delta g(m)$,$g(m-1)-g(m-2)=\Delta g(m-1)$ 和 $g(m-2)-g(m-3)=\Delta g(m-2)$. 同样地, p 整除 $\Delta^2 g(m)=\Delta g(m)-\Delta g(m-1)$ 和 $\Delta^2 g(m-1)=\Delta g(m-1)-\Delta g(m-2)$. 于是又有 $p\mid\Delta^3 g(m)=\Delta^2 g(m)-\Delta^2 g(m-1)$. 但是 $\Delta^3 g(X)=6ad^2$. 若又有 $p\mid g(0)=x_0y_0$, 则 $p\mid\gcd(x_0y_0,6ad)=1$, 这是不可能的. 于是条件 (*) 成立. 由 (H) 知存在无穷多自然数 m, 使得 $f_1(m)=p$ 和 $f_2(m)=q$. 再由 $af_1(X)^2+bf_1(X)+c=df_2(X)$, 可知 $ap^2+bp+c=dp$.

□

命题 (H_2) 又可推出:

(H_3) *每个有理数 $r>1$, 都可以用无穷多方式表成 $r=(p^2-1)/(q-1)$, 其中 p 和 q 为素数.*

证明 $(H_2)\Rightarrow(H_3)$. 令 $r=d/a$, $d>a>0$. 在命题 (H_2) 中取 $b=0,c=d-a$. 由于 $b^2-4ac=-4a(d-a)<0$, 它不是平方数. 令 $x_0=y_0=1$, 则 (H_2) 中条件成立. 于是有无穷多素数对 p,q, 使得 $ap^2+bp+c=dq$. 即

$$\frac{d}{a}=\frac{d}{a}q-p^2+1,\qquad r=\frac{p^2-1}{q-1}.$$ □

现在回到一开始叙述的命题

(H_4) *存在无穷多正整数组 (a,b,c) 使得 $a^2+b^2=c^2$ 并且 a*

和 c 为素数.

证明 $(H_3) \Rightarrow (H_4)$. 令 $r=2$, 则存在无穷多对素数 p,q, 使得 $2=(p^2-1)/(q-1)$. 于是 $p^2=2q-1$, 而 $p^2+(q-1)^2=q^2$. □

三角形 $(3,4,5)$ 和 $(5,12,13)$ 是上述意义下的 2- 素边直角三角形，它们与素数 5 相联系. Dubner 于 1999 年告诉我，他研究下面的问题.

我引进 Dubner 链这一概念：这是 (有限或无限的)2- 素边直角三角形序列, 并且每个三角形都和下一个三角形有公共边. 到目前为止，我不知是否由猜想 (H) 可推出任意长的 Dubner 链的存在性.

若 $a^2+b^2=c^2$, 并且 a 为素数，则 (a,b,c) 必是本原的，于是 $a=u^2-v^2$, $b=2uv$, $c=u^2+v^2$. 由 a 是素数，可知 $u-v=1$. 于是 $b=2v^2+2v$, $c=2v^2+2v+1$. 因此 $c=b+1$, 和证明 $(H_3) \Rightarrow (H_4)$ 中的情形一致. 所以当 a 增大时，Dubner 链中的三角形越来越细长. 又由于 $a^2=(u+v)^2=c+b=2c-1$, 所以需要求素数 a, 使得 $c=(a^2+1)/2$ 也是素数.

对于 $k=2,3,4,5,6$,Dubner 决定了产生长 k 的链的最小素数 a. 它们为

k	产生 k 个三角形的最小 a
2	3
3	271
4	169219
5	356498179
6	2500282512131

很难构作长的直角三角形链，使最长的两边都是素数. Dubner 和 Forbes(2001) 构作了一个长为 7 的 Dubner 链，其中 $a=2185103796349763249$, 而最后一个三角形的斜边是 2310 位的

素数 c.

P.T.Mielke 告诉我 (H_3) 有以下的推论，它涉及整数边的三角形，但不必是直角三角形.

(H_5) *存在无穷多整数边长 a,p,q 的三角形，其中 p 和 q 都是素数，而边 a 和 p 之间的夹角为 $\pi/3$(或为 $2\pi/3$).*

证明 $(H_3) \Rightarrow (H_5)$. 由 (H_3) 知存在无穷多素数对 (p,q), 使得 $4 = (p^2-1)/(q-1)$. 这时 $p > 2$ 并且 $q = (p^2+3)/4$. 令 $a = (p-1)(p+3)/4$, 则 a 为整数而 $a-p = (p+1)(p-3)/4$, 并且

$$p^2+a^2-ap = p^2+a(a-p) = p^2+\frac{(p^2-1)(p^2-q)}{16} = \left(\frac{p^2+3}{4}\right)^2 = q^2$$

由余弦定理，这意味着边 a 和 p 之间的夹角为 $\pi/3$. 若取 $a = (p+1)(p-3)/4$, 则类似可证夹角为 $2\pi/3$. □

Sierpiński 在 1958 年那篇文章中提出下列猜想：

(S) *对每个整数 $n>1$, 将 n^2 个整数 $1,2,\cdots,n^2$ 写成 $n\times n$ 方阵*

$$\begin{array}{cccc} 1 & 2 & \cdots & n \\ n+1 & n+2 & \cdots & 2n \\ 2n+1 & 2n+2 & \cdots & 3n \\ \vdots & \vdots & & \vdots \\ (n-1)n+1 & (n-1)n+2 & \cdots & n^2 \end{array}$$

则每行均有素数.

2 当然在第 1 行中. 由 Bertrand 和切比雪夫定理，第 2 行也有素数. 利用 Bertrand 和切比雪夫定理的改进结果，可以对前几行有进一步的结论. 例如 Breusch 在 1932 年证明了：当 $n > 48$ 时，在 n 和 $(9/8)n$ 之间存在素数. 所以若 $0 < k \leqslant 7$ 和 $n \geqslant 9$, 则

有素数 p 满足 $kn+1 \leqslant p \leqslant (9/8)(kn+1) \leqslant (k+1)n$. 即在前 8 行均有素数.

由素数定理，对每个 $h \geqslant 1$ 均存在 $n_0 = n_0(h) > h$, 使得当 $n \geqslant n_0$ 时，存在素数 p 满足 $n < p < (1+1/h)n$. 由此可知，当 $n \geqslant n_0$ 时上述方阵前 h 行中每行均有素数.

就像前面的猜想一样，(S) 也有一些有趣的推论.

(S_1) 对每个 $n \geqslant 1$, 至少有两个素数 p 和 p', 使得 $n^2 < p < p' < (n+1)^2$.

(S_2) 对每个 $n \geqslant 1$, 至少有 4 个素数 p, p', p'', p''', 使得 $n^3 < p < p' < p'' < p''' < (n+1)^3$.

在不假设 (S) 的条件下，(S_1) 和 (S_2) 均未被证明. 但是容易证明对充分大的 n, 在 n^3 和 $(n+1)^3$ 之间存在素数 p. 这可利用 Ingham 的以下结果：对每个 $\varepsilon > 0, d_n = p_{n+1} - p_n = O\big(p_n^{(5/8)+\varepsilon}\big)$.

Schinzel 把 Sierpiński 猜想变成以下形式：

(S') 对每个整数 $n > 1$, 像 (S) 那样将 n^2 个整数 $1, 2, \cdots, n^2$ 排成 n 阶方阵. 如果 $1 \leqslant k \leqslant n$, $\gcd(k, n) = 1$, 则方阵的第 k 列包含素数.

Schinzel 和 Sierpiński 没有谈及猜想 (S') 的任何推论. 我想这一定是在星期日晚上，他们太累了. 而在 1963 年，Kanold 又讲到这个猜想.

最后我介绍 Schinzel 和 Sierpiński 文章中的一个评论：

> 我们不知道我们猜想的命运如何，但是我们想，既使这些猜想被否定，对于数论也是有益的.

6.3 连续取多个合成数值的多项式

现在介绍 McCurley 的一些有趣结果. 根据 Bouniakowsky 猜想, 若 $f(X)$ 是整系数不可约多项式, 并且满足条件 (*), 则存在最小的整数 $m \geqslant 1$, 使得 $f(m)$ 为素数. 这个最小正整数 m 表示成 $p(f)$.

若 $f(X) = dX + a$, 其中 $d \geqslant 2$, $1 \leqslant a \leqslant d-1$, $\gcd(a, d) = 1$, 当然 $p(f)$ 是存在的. 用第四章 4.4 节的记号

$$p(dX + a) = \frac{p(d, a) - a}{d}$$

而 Prachar 和 Schinzel 曾给出 $p(d, a)$ 的下界.

McCurley 把上述结果推广到任意次数的多项式 $f(X)$. 他所用的一个重要工具是 Odlyzko 的下面结果 (在我第二章引用的 Adleman,Pomerance 和 Rumely(1983) 一文中):

存在绝对常数 $C > 0$ 和无穷多个整数 $d > 1$, 使得 d 有至少 $\mathrm{e}^{C \lg d/(\lg\lg d)}$ 个形如 $p-1$ (p 为奇素数) 的因子.

对于上述的 d, 设 $p_1, \cdots, p_r$ 为奇素数, 使得 $p_i - 1$ 均整除 d. 记 $k = p_1p_2\cdots p_r - 1$ 或者 $k = 3p_1p_2\cdots p_r - 1$, 使得 $k \equiv 1 \pmod 4$. 令 $f(X) = X^d + k$, 则 $f(X)$ 不可约并且满足 (*). 由此 McCurley 在 1984 年证明了:

存在常数 $C' > 0$, 使得整数 m 满足 $|m| < \mathrm{e}^{C' \lg d/(\lg\lg d)}$ 时, $f(m)$ 为合成数.

注意证明没有明显地给出多项式来. 但通过计算机寻找, 发现了以下表 6.1 中的多项式 (第一个例子来自 Shanks 1971): 后一个多项式的最小素数取值多于 70 位.

1986 年 McCurley 用另外方法证明了:

表 6.1 具有许多初始合成数值的多项式

$f(X)$	m 小于此数时 $f(m)$ 为合成数
X^6+1091	3905
$X^6+82991$	7979
$X^{12}+4094$	170624
$X^{12}+488669$	616979

对每个 $d \geqslant 1$, 存在满足条件 (*) 的 d 次不可约多项式 $f(X)$, 使得当

$$|m| < \mathrm{e}^{C\sqrt{L(f)/(\lg L(f))}}$$

时, $|f(m)|$ 为合成数.

这里 $L(f)$ 是 $f(X)=\sum\limits_{k=0}^{d} a_k X^k$ 的长度,定义为 $L(f)=\sum\limits_{k=0}^{d}\|a_k\|$, 而 $\|a_k\|$ 是 $|a_k|$ 的二进制展开时的位数, $\|0\|=1$. 这个结果可用于任何次数的多项式, 并且证明中明显地给出具有所需性质的多项式.

对于某些情形 McCurley 决定出 $p(X^d+k)$. 以下表 6.2 是他所列表中的一部分:

表 6.2 具有许多初始合成数取值的多项式 X^d+k

d	m	$\max\{p(X^d+k) \mid k \leqslant m\}$
2	10^6	$p(X^2+576239)=402$
3	10^6	$p(X^3+382108)=297$
4	150000	$p(X^4+72254)=2505$
5	10^5	$p(X^5+89750)=339$

S.M.Williams 考虑首项系数不为 1 的二次多项式, 1992 年他

告诉我以下结果:

$$
\begin{aligned}
P(8X^2+X+564135) &= 482 \\
P(4X^2+X+530985) &= 472 \\
P(2X^2+X+931650) &= 443 \\
P(73X^2+7613) &= 420
\end{aligned}
$$

6.4 数的分拆

仔细研究 Hardy 和 Littlewood(1923) 的文章“数的分拆 III：数表成素数之和”是非常有益的. 在这里会看到在从未有过的范围内一种理性的系统尝试, 对于满足各种附加条件的素数的分布给出经验公式.

我将从 Hardy 和 Littlewood 文章中选取几个概率猜想 (由于这些猜想已成为经典, 我保持它们的标号). 第一个猜想是关于哥德巴赫问题:

猜想 A *每个充分大的偶数 $2n$ 均为两个素数之和. 其表法的渐近公式为*

$$
r_2(2n) \sim C_2 \frac{2n}{(\lg 2n)^2} \prod_{\substack{p>2 \\ p\mid n}} \frac{p-1}{p-2}
$$

其中

$$
C_2 = \prod_{p>2}\left(1-\frac{1}{(p-1)^2}\right) = 0.66016\cdots
$$

注意 C_2 和第四章 4.3 节的孪生素数常数是一样的.

下面猜想涉及相差为给定值 $2k$ 的素数 (不必相邻), 所以特别地包括孪生素数情形:

猜想 B 对于每个偶数 $2k \geqslant 2$, 均存在无穷多个素数 p, 使得 $p+2k$ 也是素数. 对于 $x \geqslant 1$, 令

$$\pi_{X,X+2k}(x) = \#\{素数p \mid p+2k为素数并且\ p+2k \leqslant x\}$$

则

$$\pi_{X,X+2k} \sim 2C_2 \frac{x}{(\lg x)^2} \prod_{\substack{p>2 \\ p \mid k}} \frac{p-1}{p-2}$$

其中 C_2 是孪生素数常数.

特别若 $2k=2$, 这给出第四章 4.3 节已指出过的孪生素数渐近公式.

猜想 E 是关于形如 m^2+1 的素数.

猜想 E 存在无穷多个形如 m^2+1 的素数. 对于 $x \geqslant 1$, 令

$$\pi_{X^2+1}(x) = \#\{素数p \leqslant x \mid p = m^2+1\}$$

则

$$\pi_{X^2+1}(x) \sim \mathrm{C}\frac{\sqrt{x}}{\lg x}$$

其中

$$\mathrm{C} = \prod_{p \geqslant 3}\left(1 - \frac{(-1 \mid p)}{p-1}\right) = 1.37281346\cdots$$

而 $(-1 \mid p) = (-1)^{(p-1)/2}$ 是勒让德符号.

从表 6.3 可以看出, 猜想给出的值和 $\pi_{X^2+1}(x)$ 的实际值非常符合 (后两行是 Wunderlich 在 1973 年计算的):

表 6.3　形如 m^2+1的素数

x	$\pi_{X^2+1}(x)$	$C\sqrt{x}\log x$	比值
10^6	112	99	0.8839
10^8	841	745	0.8858
10^{10}	6656	5962	0.8957
10^{12}	54110	49684	0.9182
10^{14}	456362	425861	0.9332

这里我要提到 Iwaniec(1978) 的结果: 存在无穷多个形如 m^2+1 的 2- 殆素数.

下面又是一个猜想.

猜想 F　设 $a>0$, b 和 c 为整数, $\gcd(a,b,c)=1$,b^2-4ac 不是平方数, 并且 $a+b$ 和 c 不同时为偶数. 则有无穷多个形如 am^2+bm+c 的素数 (这是命题 (B_1)), 并且不超过 x 的上述形式的素数个数有渐近式

$$\pi_{aX^2+bX+c}(x)\sim\frac{\varepsilon C}{\sqrt{a}}\frac{\sqrt{x}}{\lg x}\prod_{\substack{p>2\\ p\mid\gcd(a,b)}}\frac{p}{p-1}$$

其中

$$\varepsilon=\begin{cases}1, & 2\nmid a+b\\ 2, & 2\mid a+b\end{cases}$$

$$C=\prod_{\substack{p>2\\ p\nmid a}}\left(1-\frac{((b^2-4ac)\mid p)}{p-1}\right)$$

其中 $((b^2-4ac)\mid p)$ 是勒让德符号.

特别地, 猜想可用于形如 m^2+k 的素数, 其中 $-k$ 不是平方数.

特别对多项式 $f_A(X)=X^2+X+A(A\geqslant 1$ 为整数), 猜想 F 为

$$\pi_{X^2+X+A}(x)\sim C(A)\frac{2\sqrt{x}}{\lg x}$$

其中

$$C(A)=\prod_{p>2}\left(1-\frac{((1-4A)\mid p)}{p-1}\right)$$

注意对多项式 $f_A(X)$, 第三章定义的

$$\pi^*_{f_A(X)}(N)=\pi^*_{X^2+X+A}(N)=\#\{n\leqslant N\mid f_A(n)\text{为素数}\}$$

与 $\pi_{f_A(X)}(N^2)$ 很近

$$\pi^*_{X^2+X+A}(N)\sim\pi_{X^2+X+A}(N^2)\sim C(A)\frac{N}{\lg N}$$

所以 $C(A)$ 值越大, 素数个数 $\pi^*_{X^2+X+A}(N)$ 可能越大.

Shanks(1975) 对于 $A=41$(即欧拉的著名多项式) 算出 $C(41)=3.3197732$.Fung 和 Williams 在 1990 年对于许多 A 算出 $C(A)$ 和 $\pi^*_{X^2+X+A}(10^6)$.Jacobson(1995) 又作了范围更大的计算.

记录

到目前为止的计算工作, 对某个 70 位的整数 A, 得到最大值 $C(A)=5.5338891$, 这是 Jacobson 和 Williams 在 2003 年发表的. Jacobson 在他 1995 年论文中得到

$$C(517165153168577)=5.0976398$$

由此得到

$$\pi^*_{X^2+X+517165153168577}(10^6)=300923$$

在此之前的记录是 Fung 和 Williams 给出的

$$C(132874279528931) = 5.0870883$$

$$\pi^*_{X^2+X+132874279528931}(10^6) = 312975$$

目前得到的 $\pi^*_{X^2+X+A}(10^6)$ 的最大值为

$$\pi^*_{X^2+X+21425625701}(10^6) = 361841$$

其中

$$C(21425625701) = 4.7073044$$

作为比较，我们有

$$\pi^*_{X^2+X+41}(10^6) = 261081, \qquad C(41) = 3.3197732$$

N.G.W.H.Beeger 在 1939 年给出

$$\pi^*_{X^2+X+27941}(10^6) = 286129, \qquad C(27941) = 3.6319998$$

《数的分拆》中还有许多其他猜想. 这里我只打算再提一个:

猜想 N *存在无穷多个形如 $p = k^3 + l^3 + m^3$ 的素数，其中 k, l, m 均是正整数.*

猜想还对可以这样表示的 x 以内素数个数建议了一个渐近估计式.

Heath-Brown 于 2001 年证明了如下定理:

存在无穷多个形如 $p = k^3 + 2l^3$ 的素数，其中 k, l 为正整数.

由此推出猜想 N 成立，但是证明方法得不到猜想的渐近估计式. 立方和问题比平方和问题要困难许多，所以 Heath-Brown 定理是 2 项型表达素数问题的一个重大的进步.

人们对于 Hardy 和 Littlewood 的各种猜想作了大量计算，试图精确决定公式中的常数，验证与实际观察结果符合的程度. 由于常数多半是表达式收敛很慢的无穷乘积，有人把这些表达式加以变型使其更容易计算.



附　录　1

素数和配对 (M.Ra,Murty)

组合学中有一个著名的定理, 即由 Philip Hall 于 1935 年证明的联姻定理. 它的内容为：若 X 是二分图, 顶点分成 U 和 V 两个部分, 则存在 U 中元与 V 中元之间的一个配对当且仅当对于 U 的每个子集合 S ， S 的 "邻域"(即 V 中与 S 中的某元素相邻的全部元素组成的集合) 中的元素个数不少于 S 中的元素个数. 换句话说, 我们可以在图中得到互不相交的一些边, 使得每个顶点均是其中某个边的端点.

初看起来, 这个定理似乎并不深奥, 它往往用 (其名所示的) 婚姻术语加以叙述和证明, 其中子集合 U 和 V 分别表示男人和女人, 而问题则是将他们分成配偶. 尽管它看上去简单和通俗易懂, 这个定理在组合理论中有深刻的应用. 我们这里的目的是将它与数轮中的一个著名的猜想联系起来.

1969 年， C.A.Grimm 叙述了关于相邻合成数的一个猜想. 他预言, 如果 $n+1,\cdots,n+k$ 是相邻合成数, 则存在两两不同的素数 p_i ， 使得 $p_i \mid n+i$. 这可以用配对的语言加以叙述. 考虑如下的二分图 X ，其中 U 是合成数 $n+1,\cdots,n+k$ 组成的集合, 而 V 是由 $(n+1)\cdots(n+k)$ 的全部素因子组成的集合. 我们将 $n+i$ 与 V 中的 p 相连当且仅当 $p \mid n+i$. 于是问题归结于是否有 U 的配对. 而配对存在的充分必要条件是 Hall 条件成立.

Erdös 和 Selfridge(1971) 发现要证明这个猜想是相当困难的. 因为由它可得到一些令人惊讶的推论. 其中一个推论是：在任何两

个相邻的平方数之间一定有素数. 这个猜想目前甚至用黎曼猜测也未能被证明. 由 Grimm 猜想推出它并不困难, 下面给出证明.

Grimm 猜想的一个推论为: 假如区间 $[n+1,n+k]$ 中没有素数, 则乘积 $P(n,k)=(n+1)\cdots(n+k)$ 至少有 k 个不同素因子. 这个较弱的论断也未被证明, 但是由此可推出任何两个相邻平方数之间必有素数.

定理 以 $\omega(m)$ 表示 m 的不同因子个数. 则存在常数 $C>0$, 使得当 $k\geqslant c\sqrt{n/\lg n}$ 时, $\omega(P(n,k))<k$.

证明 以 r 表示 $P(n,k)$ 中不同素因子个数, p_r 表示第 r 个素数. 由于 $P(n,k)\equiv 0(\bmod k!)$ 可知有不等式

$$(n+k)^k \geqslant P(n,k) \geqslant k! \prod_{\substack{p>k \\ p\mid P(n,k)}} p \geqslant k! \prod_{k<p\leqslant p_r} p$$

由素数定理知存在常数 $c_1>0$, 使得

$$\sum_{k<p<p_r} \lg p = p_r - k + O(p_r \mathrm{e}^{-c_1\sqrt{\lg p_r}})$$

如果 $r\geqslant k$, 则 (再由素数定理) 上式左边至少有 $k\lg k$ 并且当 $r\to\infty$ 时 $p_r\sim r\lg r + r\lg\lg r$. 由此给出

$$(n+k)^k \geqslant k!k^k(\lg k)^k$$

利用初等不等式 $\mathrm{e}^k > k^k/k!$ 可得

$$n+k>\left(\frac{k^2}{\mathrm{e}}\right)\lg k$$

由此即得定理. □

系 由 Grimm 猜想可推出：任何两个相邻平方和之间必有素数.

证明 假设 Grimm 猜想成立并且在 $n = m^2$ 和 $n + k = (m+1)^2$ 之间没有素数，则 $k = 2m + 1$ 并且 $\omega(P(n,k)) \geqslant k$. 由上述定理知 $k = O(\sqrt{n/\lg n})$ ，而这不可能. □

不难看出在上面叙述中，每个推理都可更为明确，即所有常数都是有效的.

这个结果使我们来研究函数 $g(n)$ ，它定义成使 Grimm 猜想对区间 $(n+1, n+k)$ 成立的最大整数 k. 显然有 $g(n) < 2n$ ，因为这时区间包括有 2 的两个方幂. 上面定理给出

$$g(n) = O(\sqrt{n/\lg n})$$

所以给出 $g(n)$ 的上下界是一个有趣的研究题目. 利用联姻定理，Erdös 和 Selfridge(1971) 证明了

$$g(n) \geqslant (1 + o(1)) \lg n.$$

随后用 Baker 方法， Ramachandra, Shorey 和 Tijdeman(1975) 证明了

$$\frac{(\lg n)^2}{(\log_2 n)^5 (\log_3 n)^2} = O(g(n)).$$

我们现在指出 Erdös 和 Selfridge 所用的推导. 但首先给出由联姻定理得到的如下推论.

引理 对每个 $n \geqslant 1$ ，在区间 $[n+1, n+g(n)+1]$ 中有 $s+1$ 个不同整数，使它们的乘积 T 有 s 个不同素因子，并且 T 的最大素因子小于 $g(n)$.

证明 构作二分图，其两部分顶点分别为区间中所有整数和区间内所有整数之乘积的全部素因子．将区间中每个整数与它的所有素因子相连．由 $g(n)$ 的定义可知 Hall 条件对此图不成立．所以区间中必有 $s+1$ 个不同的整数，它们最多与 s 个素数相邻．取 s 为具有此性质的最小整数，则区间中任何 s 个整数之积都至少有 s 个不同素因子．于是 T 恰好有 s 个不同的素因子．设 T 有素因子 $p>g(n)$，则 p 整除 $[n+1,n+g(n)+1]$ 中的某个 n_j．由于区间长度为 $g(n)$，可知区间中没有别的整数被 p 整除．现在 T/n_j 是 s 个整数之积并且至多有 $s-1$ 个素因子．由 s 的最小性质，T/n_j 至少有 s 个素因子，这导致矛盾． □

定理 (Erdös 和 Selfridge) $g(n) \geqslant (1+o(1)) \lg n$.

证明 由上述引理，可取整数 $n_1,\cdots,n_{s+1}$，使它们的乘积 T 恰有 s 个素因子．对每个 $p \mid T$，记 a_p 为诸 n_i 中被 p 的幂整除的最大方幂，取诸 n_i 中的元素 m_p 使得 $p^{a_p} \mid m_p$．由于 T 有 s 个素因子，由鸽笼原理，有某个 n_k 不是上述 s 个 m_p．考虑因子分解

$$n_k = \prod_{p \mid T} p^{e_p}$$

则 $e_p \leqslant a_p$．于是 p^{e_p} 同时除尽 n_k 和 m_p．于是 $p^{e_p} \mid |n_k - m_p| \leqslant g(n)$．所以 $n \leqslant n_k \leqslant g(n)^s$，即 $s \geqslant \lg n / \lg g(n)$．但是 T 的所有素因子都小于等于 $g(n)$．于是 $s \leqslant \pi(g(n))$．由素数定理，有

$$s \leqslant (1+o(1)) \frac{g(n)}{\lg g(n)}$$

将以上事实放到一起，给出

$$g(n) \geqslant (1+o(1)) \lg n$$

这就完成了证明. □

Ramachandra, Shorey 和 Tijdeman 证明了：对每个 $\varepsilon > 0$ 均有 $(\lg n)^{3-\varepsilon} = O(g(n))$.Cramér 一个著名猜想是说：相邻素数之差 $d_n = p_{n+1} - p_n$ 为 $O((\lg p_n)^2)$. 所以由 Cramér 猜想可推出 Grimm 猜想.



附　录　2

关于素数定理的一些可能会获得奖的工作(由 Paul T.Bateman 建议):

1. 切比雪夫 (Pavnuty L.Tschebycheff) 两篇文章: Sur la fonction qui détermine la totalité des nombres premiers inférieurs à une limite donnée, *Journal de Math.*17 (1852), 341~365; Mémoire sur les nombres premiers, *Journal de Math.* 17 (1852), 366~390.

2. 黎曼 (Bernhard Riemann) 的文章 Über die Anzahl der Primzahlen unter einer gegebenen Grösse, *Monatberichte der Königlichen Preussischen Akademie der Wissenschaften zu Berlin aus dem Jahre* 1859 (1860), 671~680.

3. 阿达玛 (Jacques Hadamard) 的两篇文章: Étude sur les propriétés des fonctions entières et en particulier d'une fonction considérée par Riemann, *Journal de Math.* 9 (1893), 171~215; Sur la distribution des zéros de la fonction $\varsigma(s)$ et ses conséquences arithmétiques, *Bulletin de la Soc.Math.de France* 24 (1896), 199 ~ 220.

4. 德拉 · 瓦累 · 布桑 (Charles-Jean de la Vallée Poussin) 的两篇文章: Recherches analytiques sur la théorie des nombres premiers; Premiére partie: La fonction $\varsigma(s)$ de Riemann et les nombres

premiers en général, *Annales de la Soc. Scientifique de Bruxelles* 20 (1896), 183~256: Sur la fonction $\varsigma(s)$ de Riemann et le nombre des nombres premiers inférieurs à une limite donnée *Mémoires couronnés et autres mémoires publiés par l'Acad. Royale des Sciences, des Lettres et des Beaux-Arts de Belgique* 59, No.1, 1899 ~ 1900, 74.

5. 郎道 (Edmund Landau) 论文 Neuer Beweis des Primzahlsatzes und Beweis des Primidealsatzes, *Math.Annalen* 56 (1903), 645 ~ 670; Über die Wurzeln der Zetafunktion, *Math.Zeitschrift* 20(1924), 98~ 104. 他的书 *Handbuch der Lahre von der Verteilung der Primzahlen*, Teubner , Leipzig, 1909, 和文章

6. 里特伍德 (John E.Littlewood) 对于分析和素数分布理论的许多贡献. 特别是他的两篇文章 Quelques conséquences de l'hypothèse que la foncton $\varsigma(s)$ de Riemann n'a pas de zéros dans le demiplan $\mathrm{RE}(s) > \frac{1}{2}$,*Comptes Rendus de l'Acad.des Sciences*, Paris, 154 (1912), 263~266; Sur la distribution des nombres premiers, *Comptes Rendus de l'Acad.des Sciences*, Paris, 158 (1914), 1869~1872. 他与哈迪 (G.H.Hardy) 合作论文 " Contributions to the theory of the Riemann zeta function and the theory of the distribution of primes ", *Acta Math.* 41 (1917), 119~196. 以及他关于 ς- 函数和 L- 函数的工作.

7.1933 年 Bôcher 奖获得者维纳 (Norbert Wiener) 的长篇文章 " Tauberian theorems ", *Annals of Math.* (2)33(1932), 1~100.

8. 维诺格拉多夫 (Ivan M. Vinogradov) 关于指数和的工作，特别是他的三篇文章 "On Weyl's sums", *Mat.Sbornik* 42 (1935), 521~529; A new method of resolving certain general questions of the theory of numbers, *Mat.Sbornik* 43 (1936), 9~19; "A new method of estimation of trigonometrical sums", *Mat.Sbornik* 43(1936),175 ~ 188.

9. 伯令 (Arne Beurling) 的文章 " Analyse de la loi asymptotique de la distribution des nombres premiers généralisés ", *Acta Math.* 68(1937), 255~291.

10. 塞尔伯格 (Atle Selberg) 对于 zeta 函数和素数分布理论的贡献. 特别是他的文章 "An elementary proof of the prime number theorem", *Annals of Math.* (2) 50 (1949), 305~313.

11.1951 年 Cole 奖获得者埃尔多斯 (Paul Erdös) 关于数论的许多工作, 特别是他的文章 " On a new method in elementary number theory which leads to an elementary proof of the prime number theorem ", *Proceedings of the National Acad.of Sciences of the U.S.A.* 35 (1949), 374~385.

12. 纽曼 (Donald J.Newman) 对分析和数论的贡献. 特别是他的文章 " Simple analytic proof of the prime number theorem ", *The American Math.Monthly* 87 (1980), 603~696.

参 考 文 献

一般性参考书

1909 Landau, E. *Handbuch der Lehre von der Verteilung der Primzahlen.* Teubner, Leipzig, 1909. Reprinted by Chelsea, Bronx, NY, 1974.

1927 Landau, E. *Vorlesungen über Zahlentheorie(in 3 volumes).* S. Hirzel, Leipzig, 1927. Reprinted by Chelsea, Bronx, NY, 1969.

1938 Hardy, G. H. & Wright, E. M. *An Introduction to the Theory of Numbers.* Clarendon Press, Oxford, 1938 (5th edition, 1979).

1952 Davenport, H. *The Higher Arithmetic.* Hutchinson, London, 1952 (7th edition, Cambridge Univ. Press, Cambridge, 1999).

1953 Trost, E. *Primzahlen.* Birkhäuser, Basel, 1953 (2nd edition, 1968).

1957 Prachar, K. *Primzahlverteilung.* Springer-Verlag, Berlin, 1957 (2nd edition, 1978).

1962 Shanks, D. *Solved and Unsolved Problems in Number Theory.* Spartan, Washington, 1962 (3rd edition by Chelsea, Bronx, NY, 1985).

1963 Ayoub, R. G. *An Introduction to the Analytic Theory of Numbers.* Amer. Math. Soc. Providence, RI, 1963.

1964 Sierpiński, W. *Elementary Theory of Numbers.* Hafner, New York, 1964 (2nd edition, North-Holland, Amsterdam, 1988).

1974 Halberstam, H. & Richert, H. E. *Sieve Methods.* Academic Press, New York, 1974.

1975 Ellison, W. J. & Mendès-France, M. *Les Nombres Premiers.* Hermann, Paris, 1975.

1976 Adams, W. W. & Goldstein, L. J. *Introduction to Number Theory.* Prentice-Hall, Englewood Cliffs, NJ, 1976.

1981 Guy, R. K. *Unsolved Problems in Number Theory.* Springer-Verlag, New York, 1981 (2nd edition, 1994).

1982 Hua, L. K. *Introduction to Number Theory.* Springer-Verlag, New York, 1982.

另外一些参考书

1984 Schroeder, M. R. *Number Theory in Science and Communication.* Springer-Verlag, Berlin, 1984 (3rd edition, 1997).

1994 Crandall, R. E. *Projects in Scientific Computation.* Springer-Verlag, New York, 1994.

1996 Bach, E. & Shallit, J. *Algorithmic Number Theory, Vol 1: Efficient Algorithms.* MIT Press, Cambridge, MA, 1996.

2000 Narkiewicz, W. *The Development of Prime Number Theory.* Springer-Verlag, Berlin, 2000.

2001 Grandall, R. & Pomerance, C. *Prime Numbers. A Computational Perspective.* Sp-ringer-Verlag, New York, 2001.

第一章参考文献

1878 Kummer, E. E. Neuer elementarer Beweis des Satzes, dass die Anzahl aller Primzahlen eine unendliche ist. *Monatsber. Akad. d. Wiss.* , Berlin, 1878/9, 777 ~ 778.

1890 Stieltjes, T. J. Sur la théorie des nombres. Étude bibliographique. *Ann. Fac. Sci. Toulouse,* 4 (1890), 1 ~ 103.

1891 Hurwitz, A. *Übungen zur Zahlentheorie,* 1891 ~ 1918 (edited by H. Funk and B. Glaus). E. T. H. , Zürich, 1993.

1897 Thue, A. Mindre meddelelser II. Et bevis for at primtalleness antal er unendeligt. *Arch. f. Math. og Naturv.,* Kristiania, 19, No. 4, 1897, 3 ~ 5. Reprinted in *Selected Mathematical Papers* (edited by T. Nagell, A. Selberg and S. Selberg), 31 ~ 32. Universitesforlaget, Oslo, 1977.

1924 Pólya, G. & Szegö, G. *Aufgaben und Lehrsätze aus der Analysis,* 2 vols. Springer-Verlag, Berlin, 1924 (4th edition, 1970).

1947 Bellman, R. A note on relatively prime sequences. *Bull. Amer. Math. Soc.* 53 (1947), 778 ~ 779.

1955 Furstenberg, H. On the infinitude of primes. *Amer. Math. Monthly* 62 (1955), p. 353.

1959 Golomb, S. W. A connected topology for the integers. *Amer. Math. Monthly* 66 (1959), 663 ~ 665.

1963 Mullin, A. A. Recursive function theory (A moden look on an Euclidean idea). *Bull. Amer. Math. Soc.* 69 (1963), p. 737.

1964 Edwards, A. W. F. Infinite coprime sequences. *Math. Gazette* 48 (1964), 416 ~ 422.

1967 Samuel, P. *Théorie Algébrique des Nombres.* Hermann, Paris, 1967. English translation published by Houghton-Mifflin, Boston, 1970.

1968 Cox, C. D. & van der Poorten, A. J. On a sequence of prime numbers. *J. Austr. Math. Soc.* 8 (1968), 571 ~ 574.

1972 Borning, A. Some results for $k! \pm 1$ and $2 \cdot 3 \cdots \cdot p \pm 1$. *Math. Comp.* 26 (1972), 567 ~ 570.

1975 Guy, R. K. & Nowakowski, R. Discovering primes with Euclid. *Delta* 5 (1975), 49 ~ 63.

1980 Templer, M. On the primality of $k! + 1$ and $2 * 3 * 5 * \cdots * p + 1$. *Math. Comp.* 34 (1980), 303 ~ 304.

1980 Washington, L. C. The infinitude of primes via commutative algebras. Unpublished manuscript.

1982 Buhler, J. P. , Crandall, R. E. & Penk, M. A. Primes of the form $n! \pm 1$ and $2 \cdot 3 \cdot 5 \cdots p \pm 1$. *Math. Comp.* 38 (1982), 639 ~ 643.

1984 Naur, T. Mullin's sequence of primes is not monotonic. *Proc. Amer. Math. Soc.* 90 (1984), 43 ~ 44.

1985 Odoni, R. W. K. On the prime divisors of the sequence $w_{n+1} = 1 + w_1 w_2 \cdots w_n$. *J. London Math. Soc.* (2) 32 (1985), 1 ~ 11.

1987 Dubner, H. Factorial and primorial primes. *J. Recr. Math.* 19 (1987), 197 ~ 203.

1991 Shanks, D. Euclid's primes. *Bull. Inst. Comb. and Appl.* 1 (1991), 33 ~ 36.

1993 Caldwell, C. & Dubner, H. Primorial, factorial, and multifactorial primes. *Math. Spectrum* 26 (1993/4), 1 ~ 7.

1993 Wagstaff, Jr. , S. S. Computing Euclid's primes. *Bull. Inst. Comb. and Appl.* 8 (1993), 23 ~ 32.

1995 Caldwell, C. On the primality of $n! + 1$ and $2 \times 3 \times 5 \times \cdots \times p \pm 1$. *Math. Comp.* 64 (1995), 889 ~ 890.

2000 Narkiewicz, W. *The Development of Prime Number Theory.* Springer-Verlag, Berlin, 2000.

2002 Caldwell, C. & Gallot, Y. On the primality of $n! \pm 1$ and $2 \times 3 \times 5 \times \cdots \times p \pm 1$. *Math. Comp.* 71 (2002), 441 ~ 448.

第二章参考文献

1801 Gauss, C. F. *Disquisitiones Arithmeticae.* G. Fleischer, Leipzig, 1801. English translation by A. A. Clarke. Yale Univ. Press, New Haven, 1966. Revised English translation by W. C. Waterhouse, Springer-Verlag, New York, 1986.

1844 Eisenstein, F. G. Aufgaben. *J. Reine Angew. Math.* 27 (1844), p. 87. Reprinted in *Mathematische Werke*, Vol. I, p. 112. Chelsea, Bronx, NY, 1975.

1852 Kummer, E. E. Über die Erganzungssätze zu den allgemeinen Reciprocitätsgesetzen. *J. Reine Angew. Math.* 44 (1852), 93 ~ 146. Reprinted in *Collected Papers* (edited by A. Weil), Vol. I, 485~538. Springer-Verlag, New York, 1975.

1876 Lucas, E. Sur la recherche des grands nombres premiers. *Assoc. Française p. l'Avanc. des Sciences* 5 (1876), 61 ~ 68

1877 Pepin, T. Sur la formule $2^{2^n}+1$. *C. R. Acad. Sci. Paris.* 85 (1877), 329 ~ 331.

1878 Lucas, E. Théorie des fonctions numériques simplement périodiques, *Amer. J. Math.* 1 (1878), 184 ~ 240, 289 ~ 321.

1878 Proth, F. Théorèmes sur les nombres premiers. *C. R. Acad. Sci. Paris* 85 (1877), 329 ~ 331.

1886 Bang, A. S. Taltheoretiske Undersøgelser *Tidskrift f. Math.* (5) 4 (1886), 70 ~ 80 and 130 ~ 137.

1891 Lucas, E. *Théorie des Nombres.* Gauthier-Villars, Paris, 1891. Reprinted by A. Blanchard, Paris, 1961.

1892 Zsigmondy, K. Zur Theorie der Potenzreste. *Monatsh. f. Math. Phys.* 3 (1892), 265 ~ 284.

1899 Korselt, A. Problème chinois. *L'Interm. des Math.* 6 (1899), 142 ~ 143.

1903 Malo, E. Nombres qui, sans être premiers, vérifient exceptionnellement une congruence de Fermat. *L'Interm. des Math.* 10 (1903), p. 88.

1904 Birkhoff, G. D. & Vandiver, H. S. On the integral divisors of $a^n - b^n$. *Annals of Math.* (2) 5 (1904), 173 ~ 180.

1904 Cipolla, M. Sui numeri composti P, che verificano la congruenza di Fermat $a^{P-1} \equiv 1$ (*mod P*). *Annali di Mathematica* (3) 9 (1904), 139 ~ 160.

1912 Carmichael, R. D. On composite numbers P which satisfy the Fermat congruence $a^{P-1} \equiv 1$ (*mod P*). *Amer. Math. Monthly* 19 (1912), 22 ~ 27.

1913 Carmichael, R. D. On the numerical factors of arithmetic forms $\alpha^n \pm \beta^n$. *Annals of Math.* (2) 15 (1913), 30 ~ 70.

1913 Dickson, L. E. Finiteness of odd perfect and primitive abundant numbers with n distinct prime factors. *Amer. J. Math..* 35 (1913), 413 ~ 422. Reprinted in *The Collected Mathematical Papers* (edited by A. A. Albert), Vol. I, 349 ~ 358. Chelsea, Bronx, NY, 1975.

1914 Pocklington, H. C. The determination of the prime or composite

nature of large numbers by Fermat's theorem. *Proc. Cambridge Phil. Soc.* 18 (1914/6), 29 ~ 30.

1921 Pirandello, L. *Il Fu Mattia Pascal.* Bemporad & Figlio, Firenze, 1921.

1922 Carmichael, R. D. Note on Euler's φ-function. *Bull. Amer. Math. Soc.* 28 (1922), 109 ~ 110.

1925 Cunningham, A. J. C. & Woodall, H. J. *Factorization of* $y^n \pm 1$, $y = 2, 3, 5, 6, 7, 10, 11,$ 12 *Up to High Powers (n).* Hodgson, London, 1925.

1929 Pillai, S. S. On some functions connected with $\varphi(n)$. *Bull. Amer. Math. Soc.* 35 (1929), 832 ~ 836.

1930 Lehmer, D. H. An extended theory of Lucas' functions. *Annals of Math.* 31 (1930), 419 ~ 448. Reprinted in *Selected Papers* (edited by D. McCarthy), Vol. I, 11 ~ 48. Ch. Babbage Res. Centre, St. Pierre, Manitoba, Canada, 1981.

1932 Lehmer, D. H. On Euler's totient function. *Bull. Amer. Math. Soc.* 38 (1932), 745 ~ 751. Reprinted in *Selected Papers* (edited by D. McCarthy), Vol. I, 319 ~ 325. Ch. Babbage Res. Centre, St. Pierre, Manitoba, Canada, 1981.

1932 Western, A. E. On Lucas' and Pepin's tests for the primeness of Mersenne's numbers. *J. London Math. Soc.* 7 (1932), 130 ~ 137.

1935 Archibald, D. C. Mersenne's numbers. *Scripta Math.* 3 (1935), 112 ~ 119.

1935 Lehmer, D. H. On Lucas's test for the primality of Mersenne numbers. *J. London Math. Soc.* 10 (1935), 162 ~ 165. Reprinted in *Selected Papers* (edited by D. McCarthy) , Vol. I, 86 ~ 89. Ch. Babbage Res. Centre, St. Pierre, Manitoba, Canada, 1981.

1936 Lehmer, D. H. On the converse of Fermat's theorem. *Amer. Math. Monthly* 43 (1936), 347 ~ 354. Reprinted in *Selected Papers* (edited by D. McCarthy) , Vol. I, 90 ~ 95. Ch. Babbage Res. Centre, St. Pierre, Manitoba, Canada, 1981.

1939 Chernick, J. On Fermat's simple theorem. *Bull. Amer. Math. Soc.* 45 (1939), 269 ~ 274.

1944 Pillai, S. S. On the smallest primitive root of a prime. *J. Indian Math. Soc.* (N. S.) 8 (1944), 14 ~ 17.

1944 Schuh, F. Can $n - 1$ be divisible by $\varphi(n)$ when n is composite? (in Dutch). *Mathamatica,* Zutphen (B) 12 (1944), 102 ~ 107.

1945 Kaplansky, I. Lucas' test for Mersenne numbers. *Amer. Math.*

Monthly 52 (1945), 188 ~ 190.

1946 Erdös, P. Problem 4221 (To solve the equation $\varphi(n) = k!$ for every $k \geqslant 1$). *Amer. Math. Monthly* 53 (1946), p. 537.

1947 Klee, V. L. On a conjecture of Carmichael. *Bull. Amer. Math. Soc.* 53 (1947), 1183 ~ 1186.

1947 Lehmer, D. H. On the factors of $2^n \pm 1$. *Bull. Amer. Math. Soc.* 53 (1947), 164 ~ 167. Reprinted in *Selected Papers* (edited by D. McCarthy), Vol. III, 1081 ~ 1084. Ch. Babbage Res. Centre, St. Pierre, Manitoba, Canada, 1981.

1948 Lambek, J. Solution of problem 4221 (proposed by P. Erdös). *Amer. Math. Monthly* 55 (1948), p. 103.

1948 Ore, O. On the averages of divisors of a number. *Amer. Math. Monthly* 55 (1948), 615 ~ 619.

1948 Steuerwald R. Über die Kongruenz $a^{n-1} \equiv 1 \ (mod\ n)$. Sitzungsber. math. -naturw. KI. Bayer. Akad. Wiss. Müchen, 1948, 69 ~ 70.

1949 Erdös, P. On the converse of Fermat's theorem. *Amer. Math. Monthly* 56 (1949), 623 ~ 624.

1949 Fridlender, V. R. On the least nth power non-residue (in Russian). *Doklady Akad. Nauk SSSR* (N. S.) 66 (1949), 351 ~ 352.

1949 Shapiro, H. N. Note on a theorem of Dickson. *Bull. Amer. Math. Soc.* 55 (1949), 450 ~ 452.

1950 Beeger, N. G. W. H. On composite numbers n for which $a^{n-1} \equiv 1 \ (mod\ n)$, for every a, prime to n. *Scripta Math.* 16 (1950), 133 ~ 135.

1950 Giuga, G. Su una presumibile proprietà caratteristica dei numeri primi. *Ist. Lombardo Sci. Lett. Rend. Cl. Sci. Mat. Nat.* (3) 14 (83), (1950), 511 ~ 528.

1950 Gupta, H. On a problem of Erdös. *Amer. Math. Monthly* 57 (1950), 326 ~ 329.

1950 Kanold, H. -J. Sätze über Kreisteilungspolynome und ihre Anwendungen auf einige zahlentheoretische Probleme, II. *J. Reine Angew. Math.* 187 (1950), 355 ~ 366.

1950 Salié, H. Über den kleinsten positiven quadratischen Nichtrest einer Primzahl. *Math. Nachr.* 3 (1949), 7 ~ 8.

1950 Somayajulu, B. S. K. R. On Euler's totient function $\varphi(n)$. *Math. Student* 18 (1950), 31 ~ 32.

1951 Beeger, N. G. W. H. On even numbers m dividing $2^m - 2$. *Amer. Math. Monthly* 58 (1951), 553 ~ 555.

1951 Morrow, D. C. Some properties of D numbers. *Amer. Math. Monthly* 58 (1951), 329 ~ 330.

1952 Duparc, H. J. A. On Carmichael numbers. *Simon Stevin* 29 (1952), 21 ~ 24.

1952 Grün, O. über ungerade vollkommene Zahlen. *Math. Zeits.* 55 (1952), 353 ~ 354.

1953 Knödel, W. Carmichaelsche Zahlen. *Math. Nachr.* 9 (1953), 343 ~ 350.

1953 Selfridge, J. L. Factors of Fermat numbers. *Math. Comp.* 7 (1953), 274 ~ 275.

1953 Touchard, J. On prime numbers and perfect numbers. *Scripta Math.* 19 (1953), 35 ~ 39.

1954 Kanold, H. -J. Über die Dichten der Mengen der vollkommenen und der befreundeten Zahlen. *Math. Zeits.* 61 (1954), 180 ~ 185.

1954 Robinson, R. M. Mersenne and Fermat numbers. *Proc. Amer. Math. Soc.* 5 (1954), 842 ~ 846.

1954 Schinzel A. Quelques théorèmes sur les fonctions $\varphi(n)$ et $\sigma(n)$. *Bull. Acad. Polon. Sci.* CI. III, 2 (1954), 467 ~ 469.

1954 Schinzel, A. Generalization of a theorem of B. S. K. R. Somayajulu on the Euler's function $\varphi(n)$. *Ganita* 5 (1954), 123 ~ 128.

1954 Schinzel, A. & Sierpiński, W. Sur quelques propriétés des fonctions $\varphi(n)$ et $\sigma(n)$. *Bull. Acad. Polon. Sci.* CI. III, 2 (1954), 463 ~ 466.

1955 Artin, E. The orders of the linear group. *Comm. Pure and Appl. Math.* 8 (1955), 355 ~ 365. Reprinted in *Collected Papers* (edited by S. Lang and J. T. Tate), 387 ~ 397. Addison-Wesley, Reading, MA, 1965.

1955 Hornfeck, B. Zur Dichte der Menge vollkommenen Zahlen. *Arch. Math.* 6 (1955), 442 ~ 443.

1955 Laborde, P. A note on the even perfect numbers. *Amer. Math. Monthly* 62 (1955), 348 ~ 349.

1956 Hornfeck, B. Bemerkung zu meiner Note über vollkommene Zahlen. *Arch. Math.* 7 (1956), p. 273.

1956 Kanold, H. -J. Über einen Satz von L. E. Dickson, II. *Math. Ann.* 131 (1956), 246 ~ 255.

1956 Schinzel, A. Sur l'équation $\varphi(x) = m$. *Elem. Math.* 11 (1956), 75 ~ 78.

1956 Schinzel, A. Sur un problème concernant la fonction $\varphi(n)$. *Czechoslovak Math. J.* 6 (81), (1956), 164 ~ 165.

1957 Hornfeck, B. & Wirsing, E. Über die Häufigkeit vollkommener Zahlen. *Math. Ann.* 133 (1957), 431 ~ 438.

1957 Kanold, H. -J. Über die Verteilung der vollkommenen Zahlen und allgemeinerer Zahlenmengen. *Math. Ann.* 132 (1957), 442 ~ 450.

1958 Erdös, P. Some remarks on Euler's φ-function. *Acta Arith.* 4 (1958), 10 ~ 19.

1958 Jarden, D. *Recurring Sequences.* Riveon Lematematika, Jerusalem, 1958 (3rd edition, Fibonacci Assoc. , San Jose, CA, 1973).

1958 Perisastri, M. A note on odd perfect numbers. *Math. Student* 26 (1958), 179 ~ 181.

1858 Schinzel, A. Sur les nombres composés n qui divisent $a^n - a$. *Rend. Circ. Mat. Palermo* (2) 7 (1958), 37 ~ 41.

1958 Sierpiński, W. Sur les nombres premiers de la forme n^n+1. *L'Enseign. Math.* (2) 4 (1958), 211 ~ 212.

1959 Rotkiewicz, A. Sur les nombres pairs n pour lesquels les nombres $a^n b - ab^n$, respectivement $a^{n-1} - b^{n-1}$ sont divisibles par n. *Rend. Circ. Mat. Palermo* (2) 8 (1959), 341 ~ 342.

1959 Satyanarayana, M. Odd perfect numbers. *Math. Student* 27 (1959), 17 ~ 18.

1959 Schinzel, A. Sur les nombres composés n qui divisent $a^n - a$. *Rend. Circ. Mat. Palermo* (2) 7 (1958), 1 ~ 5.

1959 Wirsing, E. Bemerkung zu der Arbeit über vollkommene Zahlen. *Math. Ann.* 137 (1959), 316 ~ 318.

1960 Inkeri, K. Test for primality. *Annales Acad. Sci. Fennicae,* Ser. A, I, 279, Helsinki, 1960, 19 pages. Reprinted in *Collected Papers of Kustaa Inkeri* (edited by T. Metsänkylä and P. Ribenboim), Queen's Papers in Pure and Appl. Math. 91, 1992, Queen's Univ. , Kingston, Ontario, Canada.

1961 Ward, M. The prime divisors of Fibonacci numbers. *Pacific J. Math.* 11 (1961), 379 ~ 389.

1962 Burgess, D. A. On character sums and L-series. *Proc. London Math. Soc.* (3) 12 (1962), 193 ~ 206.

1962 Crocker, R. A theorem on pseudo-primes. *Amer. Math. Monthly* 69 (1962), p. 540.

1962 Mąkowski, A. Generalization of Morrow's *D* numbers. *Simon Stevin* 36 (1962), p. 71.

1962 Schinzel, A. The intrinsic divisors of Lehmer numbers in the case of negative discriminant. *Arkiv för Mat.* 4 (1962), 413 ~ 416.

1962 Schinzel, A. On primitive prime factors of $a^n - b^n$. *Proc. Cambridge Phil. Soc.* 58 (1962), 555 ~ 562.

1962 Shanks, D. *Solved and Unsolved Problems in Number Theory.* Spartan, Washington, 1962 (3rd edition by Chelsea, Bronx, NY, 1985).

1963 Schinzel, A. On primitive prime factors of Lehmer numbers, I. *Acta Arith.* 8 (1963), 211 ~ 223.

1963 Schinzel, A. On primitive prime factors of Lehmer numbers, II. *Acta Arith.* 8 (1963), 251 ~ 257.

1963 Suryanarayana, D. On odd perfect numbers, II. *Proc. Amer. Math. Soc.* 14 (1963), 896 ~ 904.

1964 Biermann, K. -R. Thomas Clausen, Mathematiker und Astronom. *J. Reine Angew. Math.* 216 (1964), 159 ~ 198.

1964 Lehmer, E. On the infinitude of Fibonacci pseudo-primes. *Fibonacci Quart.* 2 (1964), 229 ~ 230.

1965 Erdös, P. Some recent advances and current problems in number theory. In *Lectures in Modern Mathematics,* Vol. III (edited by T. L. Saaty), 196 ~ 244. Wiley, New York, 1965.

1965 Rotkiewicz, A. Sur les nombres de Mersenne dépourvus de facteurs carrés et sur les nombres naturels n tels que $n^2 \mid 2^n - 2$. *Matem. Vesnik* (Beograd) 2 (17), (1965), 78~80.

1966 Grosswald, E. *Topics from the Theory of Numbers.* Macmillan, New York, 1966 (2nd edition, Birkhäuser, Boston, 1984).

1966 Muskat, J. B. On divisors of odd perfect numbers. *Math. Comp.* 20 (1966), 141 ~ 144.

1967 Brillhart, J. & Selfridge, J. L. Some factorizations of $2^n \pm 1$ and related results. *Math. Comp.* 21 (1967), 87 ~ 96 and p. 751.

1967 Mozzochi, C. J. A simple proof of the Chinese remainder theorem. *Amer. Math. Monthly* 74 (1967), p. 998.

1970 Lieuwens, E. Do there exist composite numbers M for which $k\varphi(M) = M - 1$ holds? *Nieuw Arch. Wisk.* (3) 18 (1970), 165 ~ 169.

1970 Parberry, E. A. On primes and pseudo-primes related to the Fibonacci sequence. *Fibonacci Quart.* 8 (1970), 49 ~ 60

1970 Suryanarayana, D. & Hagis, Jr. , P. A theorem concerning odd perfect numbers. *Fibonacci Quart.* 8 (1970), 337 ~ 346.

1971 Lieuwens, E. *Fermat Pseudo-Primes.* Ph. D. Thesis, Delft, 1971.

1971 Morrison, M. A. & Brillhart, J. the factorization of F_7. *Bull. Amer. Math. Soc.* 77 (1971), p. 264.

1971 Schönhage, A. & Strassen, V. Schnelle Multiplikation grosser Zahlen. *Computing* 7 (1971), 281 ~ 292.

1972 Hagis, Jr. , P. & McDaniel, W. L. A new result concerning the structure of odd perfect numbers. *Proc. Amer. Math. Soc.* 32 (1972), 13 ~ 15.

1972 Mills, W. H. On a conjecture of Ore. *Proc. 1972 Number Th. Conf. in Boulder,* 142 ~ 146.

1972 Ribenboim, P. *Algebraic Numbers.* Wiley-Interscience, New York, 1972 (enlarged new edition, Springer-Verlag, 2001).

1972 Rotkiewicz, A. *Pseudoprime Numbers and thier Genaralizations.* Stud. Assoc. Fac. Sci. Univ. Novi Sad, 1972.

1973 Grosswald, E. Contributions to the theory of Euler's function $\varphi(x)$. *Bull. Amer. Math. Soc.* 79 (1973), 327 ~ 341.

1973 Hagis, Jr. P. A lower bound for the set of odd perfect numbers. *Math. Comp.* 27 (1973), 951 ~ 953.

1973 Rotkiewicz, A. On pseudoprimes with respect to the Lucas sequences. *Bull. Acad. Polon. Sci.* 21 (1973), 793 ~ 797.

1974 Ligh, S. & Neal, L. A note on Mersenne numbers. *Math. Mag.* 47 (1974), 231 ~ 233.

1974 Pomerance, C. On Carmichael's conjecture. *Proc. Amer. Math. Soc.* 43 (1974), 297 ~ 298.

1974 Schinzel, A. Primitive divisors of the expression $A^n - B^n$ in algebraic number fields. *J. Reine Angew. Math.* 268/269 (1974), 27 ~ 33.

1974 Sinha, T. N. Note on perfect numbers. *Math. Student* 42 (1974), p. 336.

1975 Brillhart, J. , Lehmer, D. H. & Selfridge, J. L. New primality criteria and factorizations of $2^m \pm 1$. *Math. Comp.* 29 (1975), 620 ~ 647.

1975 Guy, R. K. How to factor a number. *Proc. Fifth Manitoba Conf. Numberical Math.* , 1975, 49 ~ 89 (Congressus Numerantium XVI, Winnipeg, Manitoba, 1975).

1975 Hagis, Jr. , P. & McDaniel, W. L. On the Largest prime divisor of an odd perfect number. *Math. Comp.* 29 (1975), 922 ~ 924.

1975 Morrison, M. A. A note on primality testing using Lucas sequences. *Math. Comp.* 29 (1975), 181 ~ 182.

1975 Pomerance, C. The second largest prime factor of an odd perfect number. *Math. Comp.* 29 (1975), 914 ~ 921.

1975 Pratt, V. R. Every prime has succinct certificate. *SIAM J. Comput.*

4 (1975), 214 ~ 220.

1975 Stewart, C. L. The greatest prime factor of $a^n - b^n$. *Acta Arith.* 26 (1975), 427 ~ 433.

1976 Buxton, M. & Elmore, S. An extension of lower bounds for odd perfect numbers. *Notices Amer. Math. Soc.* 23 (1976), p. A55.

1976 Diffie, W. & Hellman, M. E. New directions in cryptography. *IEEE Trans. on Inf. Th.* IT-22 (1976), 644 ~ 654.

1976 Erdös, P. & Shorey, T. N. On the greatest prime factor of $2^p - 1$ for a prime p, and other expressions. *Acta Arith.* 30 (1976), 257 ~ 265.

1976 Lehmer, D. H. Strong Carmichael numbers. *J. Austral. Math. Soc.* (A) 21 (1976), 508 ~ 510. Reprinted in *Selected Papers* (edited by D. McCarthy), Vol. I, 140 ~ 142. Ch. Babbage Res. Centre, St. Pierre, Manitoba, Canada, 1981.

1976 Mendelsohn, N. S. The equation $\varphi(x) = k$. *Math. Mag.* 49 (1976), 37 ~ 39.

1976 Miller, G. L. Riemann's hypothesis and tests for primality. *J. Comp. Syst. Sci.* 13 (1976), 300 ~ 317.

1976 Rabin, M. O. Probabilistic algorithms. In *Algorithms and Complexity.* (edited by J. F. Traub), 21 ~ 39. Academic Press, New York, 1976.

1976 Yorinaga, M. On a congruential property of Fibonacci numbers. Numerical experiments. Considerations and remarks. *Math. J. Okayama Univ.* 19 (1976), 5 ~ 10 and 11 ~ 17.

1977 Kishore, M. Odd perfect numbers not divisible by 3 are divisible by at least ten distinct primes. *Math. Comp.* 31 (1977), 274 ~ 279.

1977 Kishore, M. *The number of distinct prime factors for which $\sigma(N) = 2N$, $\sigma(N) = 2N \pm 1$ and $\varphi(N) \mid N - 1$.* Ph. D. Thesis, Univ. of Toledo, Ohio, 1977, 39 pages.

1977 Malm, D. E. G. On Monte-Carlo primality tests. *Notices Amer. Math. Soc.* 24 (1977), A-529, abstract 77T-A22.

1977 Pomerance, C. On composite n for which $\varphi(n) \mid n - 1$, II. *Pacific J. Math.* 69 (1977), 177 ~ 186.

1977 Pomerance, C. Multiply perfect numbers, Mersenne primes and effetive computability. *Math. Ann.* 226 (1977), 195 ~ 206.

1977 Solovay, R. & Strassen, V. A fast Monte-Carlo test for primality. *SIAM J. Comput.* 6 (1977), 84 ~ 85.

1977 Stewart, C. L. On divisors of Fermat, Fibonacci, Lucas, and Lehmer numbers. *Proc. London Math. Soc.* (3) 35 (1977), 425 ~ 447.

1977 Stewart, C. L. Primitive divisors of Lucas and Lehmer numbers. In *Transcendence Theory: Advances and Applications* (edited by A. Baker and D. W. Masser), 79 ~ 92. Academic Press, London, 1977.

1977 Williams, H. C. On numbers analogous to the Carmichael numbers. *Can. Math. Bull.* 20 (1977), 133 ~ 143.

1978 Cohen, G. L. On odd perfect numbers. *Fibonacci Quart.* 16 (1978), 523 ~ 527.

1978 Kiss, P. & Phong, B. M. On a function concerning second order recurrences. *Ann. Univ. Sci. Budapest* 21 (1978), 119 ~ 122.

1978 Rivest, R. L. Remarks on a proposed cryptanalytic attack on the M. I. T. public-key cryptosystem. *Cryptologia* 2 (1978), 62 ~ 65.

1978 Rivest, R. L. , Shamir, A. & Adleman, L. M. A method for obtaining digital signatures and public-key cryptosystems. *Comm. ACM* 21 (1978), 120 ~ 126.

1978 Williams, H. C. Primality testing on a computer. *Ars Comb.* 5 (1978), 127 ~ 185.

1978 Yorinaga, M. Numerical computation of Caemichael numbers. *Math. J. Okayama Univ.* 20 (1978), 151 ~ 163.

1979 Chein, E. Z. Non-existence of odd perfect numbers of the form $q_1^{a_1} q_2^{a_2} \cdots q_6^{a_6}$ and $5^{a_1} q_2^{a_2} \cdots q_9^{a_9}$. Ph. D. Thesis, Pennsylvania State Univ. , 1979.

1979 Lanstra, Jr. , H. W. Miller's primality test. *Inf. Process. Letters* 8 (1979), 86 ~ 88.

1980 Baillie, R. & Wagstaff, Jr. , S. S. Lucas pseudoprimes. *Math. Comp.* 35 (1980), 1391 ~ 1417.

1980 Cohen, G. L. & Hagis, Jr. , P. On the number of prime factors of n if $\varphi(n) \mid (n-1)$. *Nieuw Arch. Wisk.* (3) 28 (1980), 177 ~ 185.

1980 Hagis, Jr. , P. Outline of a proof that every odd perfect number has at least eight prime factors. *Math. Comp.* 35 (1980), 1027 ~ 1032.

1980 Monier, L. Evaluation and comparison of two efficient probabilistic primality testing algorithms. *Theoret. Comput. Sci.* 12 (1980), 97 ~ 108.

1980 Pomerance, C. , Selfridge, J. L. & Wagstaff, Jr. , S. S. The pseudoprimes to $25 \cdot 10^9$. *Math. Comp.* 35 (1980), 1003 ~ 1026.

1980 Rabin, M. O. Probabilistic algorithm for testing primality. *J. Number Theory* 12 (1980), 128 ~ 138.

1980 Wagstaff, Jr. , S. S. Large Carmichael numbers *Math. J. Okayama*

Univ. 22 (1980), $33 \sim 41$.

1980 Wall, D. W. Conditions for $\varphi(N)$ to properly divide $N-1$. In: *A Collection of Manuscripts Related to the Fibonacci Sequence* (edited by V. E. Hoggatt and M. Bicknell-Johnson), $205 \sim 208$. 18th Anniv. Vol. , Fibonacci Assoc. , San Jose, 1980.

1980 Yorinaga, M. Carmichael numbers with many prime factors. *Math. J. Okayama Univ.* 22 (1980), $169 \sim 184$.

1981 Brent, R. P. & Pollard, J. M. Factorization of the eighth Fermat number. *Math. Comp.* 36 (1981), $627 \sim 630$.

1981 Grosswald, E. On Burgess's bound for primitive roots modulo primes and an application to $\Gamma(p)$. *Amer. J. Math.* 103 (1981), $1171 \sim 1183$.

1981 Hagis, Jr. , P. On the second largest prime divisor of an odd perfect number. In *Analytic Number Theory* (edited by M. I. Knopp). Lecture Notes in Math. #899, $254 \sim 263$. Springer-Verlag, New York, 1981.

1981 Lenstra, Jr. , H. W. Primality testing algorithms (after Adleman, Rumely and Williams). In *Séminaire Bourbaki,* exposé No. 576. Lecture Notes in Math. #901, $243 \sim 257$. Springer-Verlag, Berlin, 1981.

1981 Lüneburg, H. Ein einfacher Beweis für den Satz von Zsigmondy über primitive Primtei- ler von $A^N - 1$. In *Geometries and Groups* (edited by M. Aigner and D. Jungnickel). Lecture Notes in Math. #893, $219 \sim 222$. Springer-Verlag, New York, 1981.

1982 Bent, R. P. Succinct proofs of primality for the factors of some Fermat numbers. *Math. Comp.* 38 (1982), $253 \sim 255$.

1982 Couvreur C. & Quisquater, J. J. An introduction to fast generation of large prime numbers. *Philips J. Res.* 37 (1982), $231 \sim 264$; Errata, 38 (1983), p. 77.

1982 Hoogendoorn, P. J. On a secure public-key cryptosystem. In *Computational Methods in Number Theory* (edited by H. W. Lenstra, Jr. and R. Tijdeman), Part I, $159 \sim 168$. Math. Centre Tracts #154, Amsterdam, 1982.

1982 Lenstra, Jr. , H. W. Primality testing. In *Computational Methods in Number Theory* (edited by H. W. Lenstra, Jr. and R. Tijdeman), Part I, $55 \sim 77$. Math. Centre Tracts ♯ 154, Amsterdam, 1982.

1982 Masai, P. & Valette, A. A lower bound for a counterexample in Carmichael's conjecture. *Boll. Un. Mat. Ital.* (6) 1-A (1982), $313 \sim 316$.

1982 Naur, T. *Integer Factorization.* DAIMI PB-144, Aarhus University,

1982, 129 pages.

1982 Woods, D. & Huenemann, J. larger Carmichael numbers. *Comput. Math. and Appl.* 8 (1982), 215 ~ 216.

1983 Adleman, L. M. , Pomerance, C. & Rumely, R. S. On distinguishing prime numbers from composite numbers. *Annals of Math.* (2) 117 (1983), 173 ~ 206.

1983 Brillhart, J. , Lenhmer, D. H. , Selfridge, J. L. , Tuckerman, B. & Wagstaff, Jr. , S. S. *Factorizations of* $b^n \pm 1$, $b = 2, 3, 5, 6, 7, 10, 11, 12$ *Up to High powers.* Contemporary Math. , Vol. 22, Amer. Math. Soc. , Providence, RI, 1983 (2nd edition, 1988, 3rd edition electronical only, 2002).

1983 Hagis, Jr. , P. Sketch of a proof that an odd perfect number relatively prime to 3 has at laest eleven prime factors. *Math. Comp.* 40 (1983), 399 ~ 404.

1983 Kishore, M. Odd perfect numbers not divisible by 3, II. *Math. Comp.* 40 (1983), 405 ~ 411.

1983 Naur, T. New integer factorizations. *Math. Comp.* 41 (1983), 687 ~ 695.

1983 Pomerance, C. & Wagstaff, Jr. , S. S. Implementation of the continued fraction integer factoring algorithm. *Congressus Numerantium.* 37 (1983), 99 ~ 118.

1983 Powell, B. Problem 6420 (On primitive roots). *Amer. Math. Monthly* 90 (1983), p. 60.

1983 Singmaster, D. Some Lucas pseudoprimes. *Abstracts Amer. Math. Soc.* 4 (1983), p. 197, abstract 83T-10-146.

1983 Yates, S. Titantic primes. *J. Recr. Math.* 16 (1983/4), 250 ~ 260.

1984 Cohen, H. & Lenstra, Jr. , H. W. Primality testing and Jacobi sums. *Math. Comp.* 42 (1984), 297 ~ 330.

1984 Dixon, J. D. Factorization and primality tests. *Amer. Math. Monthly* 91 (1984), 333 ~ 352.

1984 Kearnes, K. Solution of problem 6420. *Amer. Math. Monthly* 91 (1984), p. 521.

1984 Nicolas, J. L. Tests de primalité. *Expo. Math.* 2 (1984), 223 ~ 234.

1984 Pomerance, C. *Lecture Notes on Primality Testing and Factoring* (Notes by G. M. Gagola, Jr.). Math. Assoc. America, Notes No. 4, 1984, 34.

1984 Williams, H. C. An overview of factoring. In *Advances in Cryptology*

(edited by D. Chaum), 71 ~ 80. Plenum, New York, 1984.

1984 Yates, S. Sinkers of the Titanics. *J. Recr. Math.* 17 (1984/5), 268 ~ 274.

1985 Bedocchi, E. Note on conjecture on prime numbers. *Rev. Mat. Univ. Perma* (4) 11 (1985), 229 ~ 236.

1985 Fouvry, E. Théorème de Brun-Titchmarsh; application au théorème de Fermat. *Invent. Math.* 79 (1985), 383 ~ 407.

1985 Riesel, H. *Prime Numbers and Computer Methods for Factorization.* Birkhäuser, Boston, 1985 (2nd edition, 1994).

1985 Wagon, S. Perfect numbers. *Math. Intelligencer* 7, No. 2 (1985), 66 ~ 68.

1986 Kiss, P. , Phong, B. M. & Lieuwens, E. On Lucas pseudoprimes which are products of s primes. In *Fibonacci Numbers and their Applications* (edited by A. N. Philippou, G. E. Bergum and A. F. Horadam), 131 ~ 139. Reidel, Dordrecht, 1986.

1986 Wagon, S. Carmichael's " Empirical Theorem ". *Math. Intelligencer* 8, No. 2 (1986), 61 ~ 62.

1986 Wagon, S. Primality testing. *Math. Intelligencer* 8, No. 3 (1986), 58 ~ 61.

1987 Cohen, G. L. On the largest component of an odd perfect number. *J. Austral. Math. Soc.* (A) 42 (1987), 280 ~ 286.

1987 Cohen, H. & Lenstra, A. K. Implementation of a new primality test. *Math. Comp.* 48 (1987), 103 ~ 121 and S1-S4.

1987 Koblitz, N. *A Course in Number Theory and Cryptography.* Springer-Verlag, New York, 1987.

1987 Lenstra, Jr. , H. W. Factoring integers with elliptic curves. *Annals of Math.* 126 (1987), 649 ~ 673.

1987 Li Yan & Du Shiran. *Chinese Mathematics. A Concise History* (English translation by J. N. Crossley and A. W. C. Lun). Clarendon Press, Oxford, 1987.

1987 Pomerance, C. Very short primality proofs. *Math. Comp.* 48(1987), 315 ~ 322.

1988 Brillhart, J. , Montgomery, P. L. & Silverman, R. D. Tables of Fibonacci and Lucas factorization, and Supplement. *Math. Comp.* 50 (1988), 251 ~ 260 and S1-S15.

1988 Young, J. & Buell, D. A. The twentieth Fermat number is composite. *Math. Comp.* 50 (1988), 261 ~ 263.

1989 Bateman, P. T. , Selfridge, J. L. & Wagstaff, Jr. , S. S. The new Mersenne conjecture. *Amer. Math. Monthly* 96 (1989), 125 ~ 128.

1989 Brent, R. P. & Cohen, G. L. A new lower bound for odd perfect numbers. *Math. Comp.* 53 (1989), 431 ~ 437 and S7-S24.

1989 Bressoud, D. M. *Factorization and Primality Testing.* Springer-Verlag, New Yoek, 1989.

1989 Dubner, H. A new method for producing large Carmichael numbers. *Math. Comp.* 53 (1989), 411 ~ 414.

1989 Lemos, M. *Criptografia, Números Primos e Algoritmos.* 17° Colóquio Brasileiro de Matemática, Inst. Mat. Pura e Aplic. , Rio de Janeiro, 1989, 72 pages.

1990 Lenstra, A. K. & Lenstra, Jr. , H. W. Algorithms in number theory. In *Handbook of Theoretical Computer Science.* (edited by J. van Leeuwen, A. Meyer, M. Nivat, M. Paterson and D. Perrin). North-Holland, Amsterdam, 1990.

1991 Brent, R. P. , Cohen, G. L. & te Riele, H. J. J. Improved techniques for lower bounds for odd perfect numbers. *Math. Comp* 57 (1991), 857 ~ 868.

1991 Frasnay, C. Extension à l'anneau $\mathbb{Z}_p$ du théorème de Lucas, sur les coefficients binomiaux. *Singularité.* 2 (1991), 13 ~ 15.

1992 Yates, S. Collecting gigantic and titanic primes. *J. Recr. Math.* 24 (1992), 187 ~ 195.

1993 Atkin, A. O. L. & Morain, F. Elliptic curves and primality proving. *Math. Comp.* 61 (1993), 29 ~ 68.

1993 Cohen, H. *A Course in Computational Number Theory.* Springer-Verlag, New York, 1993.

1993 Jaeschke, G. On strong pseudoprimes to several bases. *Math. Comp.* 61 (1993), 915 ~ 926.

1993 Lenstra, A. K. , Lenstra, Jr. , H. W. , Manasse, M. S. & Pollard, J. M. The number field sieve. In *The Development of the Number Field Sieve* (edited by A. K. Lenstra and H. W. Lenstra, Jr.). Lecture Notes in Math. #1554, 11 ~ 42. Springer-Verlag, New York, 1993.

1993 Pomerance, C. Carmichael numbers. *Nieuw Arch. Wisk.* (4) 11 (1993), 199 ~ 209.

1993 Williams, H. C. How was F_6 factored? *Math. Comp.* 61 (1993), 463 ~ 474.

1994 Alford, W. R. , Granville, A. & Pomerance, C. There are infinitely

many Carmichael numbers. *Annals of Math.* (2) 140 (1994), 703 ~ 722.

1994 Heath-Brown, D. R. Odd perfect numbers. *Math. Proc. Cambridge Phil. Soc.* 115 (1994), 191 ~ 196.

1994 Schlafly, A. & Wagon, S. Carmichael's conjecture on the Euler function is valid below $10^{10000000}$. *Math. Comp.* 63 (1994), 415 ~ 419.

1994 Williams, H. C. & Shallit, J. O. Factoring integers before computers. In *Mathematics of Computation,* 1943 ~ 1993: *A Half Century of Computational Mathematics* (edited by W. Gautschi). Proc. Symp. Appl. Math. , Vol. 48, 481 ~ 531. Amer. Math. Soc. , Providence, RI, 1994.

1995 Crandall, R. E. , Doenias, J. , Norrie, C. & Young, J. The twenty-second Fermat number is composite. *Math. Comp.* 64 (1995), 863 ~ 868.

1995 Gostin, G. B. New factors of Fermat numbers. *Math. Comp.* 64 (1995), 393 ~ 395.

1995 McIntosh, R. J. On the converse of Wolstenholme's theorem. *Acta Arith.* 71 (1995), 381 ~ 389.

1995 Trevisan, V. & Carvalho, J. B. The composite character of the twenty-second Fermat number. *J. Supercomp.* 9 (1995), 179 ~ 182.

1996 Borwein, D. , Borwein, J. M. , Borwein, P. B. & Girgensohn, R. Giuga's conjecture on primality. *Amer. Math. Monthly* 103 (1996), 40 ~ 50.

1996 Löh, G. & Niebuhr, W. A new algorithm for constructing large Carmichael numbers. *Math. Comp.* 65 (1996), 823 ~ 836.

1998 Ford, K. The distribution of totients. *Hardy-Ramanujan J.* 2 (1998), 67 ~ 151.

1998 Hagis, Jr. , P. & Cohen, G. L. Every odd perfect number has a prime factor which exceeds 10^6. *Math. Comp.* 67 (1998), 1323 ~ 1330.

1998 Pinch, R. G. E. The Carmichael numbers up to 10^{16}. Unpublished manuscript.

1998 Williams, H. G. *Édouard Lucas and Primality Testing.* J. Wiley and Sons, New York, 1998.

1998 Young, J. Large primes and Fermat factors. *Math. Comp.* 67 (1998), 1735 ~ 1738.

1999 Brent, R. P. Factorization of the tenth Fermat number. *Math. Comp.* 68 (1999), 429 ~ 451.

1999 Cook, R. J. Bounds for odd perfect numbers. In *Number Theory* (edited by R. Gupta). CRM Proc. Lecture Notes #19, 67 ~ 71. Amer.

Math. Soc. , Providence, RI, 1999.

1999 Coutinho, S. C. *The Mathematics of Ciphers: Number Theory and RSA Cryptography.* A. K. Peters, Natick, MA, 1999.

1999 Ford, K. The number of solutions of $\varphi(x) = m$. *Annals of Math.* (2) 150 (1999), 283 ~ 311.

1999 Grytczuk, A. & Wojtowicz, M. there are no small odd perfect numbers, and Erratum. *C. R. Acad. Sci. Paris* 328 (1999), 1101 ~ 1105, and 330 (2000), p. 533.

1999 Iannucci, D. E. The second largest prime divisor of an odd perfect number exceeds ten thousand. *Math. Comp.* 68 (1999), 1749 ~ 1760.

1999 Woltman, G. On the discovery of the 38th known Mersenne prime. *Fibonacci Quart.* 37 (1999), 367 ~ 370.

2000 Brent, R. P. , Crandall, R. E. , Dilcher, K. & van Halewyn, C. Three new factors of Fermat numbers. *Math. Comp.* 69 (2000), 1297 ~ 1304.

2000 Caldwell, C. & Dubner, H. Primes in π. Preprint, 2000.

2000 Iannucci, D. E. The third largest prime divisor of an odd perfect number exceeds one hundred. *Math. Comp.* 69 (2000), 867 ~ 879.

2001 Crandall, R. E. & Pomerance, C. *Prime Numbers. A Computational Perspective.* Springer-Verlag, New York, 2001.

2001 Křížek, M. , Luca, F. & Somer, L. *17 Lectures on Fermat Numbers. From Number Theory to Geometry.* Springer-Verlag, New York, 2001.

2001 Ribenboim, P. *Classical Theory of Algebraic Numbers.* Springer-Verlag, New York, 2001.

2001 Zhang, Z. Finding strong pseudoprimes to several bases. *Math. Comp.* 70 (2001), 863 ~ 872.

2002 Agrawal, M. , Kayal, N. & Saxena, N. PRIMES is in P. Preprint, 2002.

2002 Morain, F. Primalité théorique et primalité pratique ou AKS vs. ECCP. Preprint, 2002.

2003 Bailey, D. H. Some backgroud on Kanada's recent pi calculation. Preprint, 2003.

2003 Crandall, R. E. , Mayer, E. W. & Papadopuolos, J. S. The twenty-fourth Fermat number is composite. *Math. Comp.* 72 (2003), 1555 ~ 1572.

2003 Wagstaff, Jr. , S. S. *Cryptanalysis of Number Theoretic Ciphers.* Chapman & Hall/CRC, Boca Raton, FL, 2003.

第三章参考文献

1912 Frobenius,F.G. Über quadratische Formen,die viele Primzahlen darstellen. *Sitzungsber. d. Königl. Akad. d. Wiss. zu Berlin,* 1912, 966 ~ 980. Reprinted in *Gesammelte Abhandlungen,* Vol. III, 573 ~ 587. Springer-Verlag, Berlin, 1968.

1912 Rabinowitsch, G. Eindeutigkeit der Zerlegung in Primzahlfaktoren in quadratischen Zahlkörpern. *Proc. Fifth Intern. Congress Math.* , Cambridge, Vol. 1, 1912, 418 ~ 421.

1933 Lehmer, D. H. On imaginary quadratic fields whose class number is unity. *Bull. Amer. Math. Soc.* 39 (1933), p. 360.

1934 Heilbronn, H & Linfoot, E. H. On the imaginary quadratic corpora of class-number one. *Quart. J. Pure and Appl. Math.* , Oxford, (2) 5 (1934), 293 ~ 301.

1936 Lehmer, D. H. On the function $x^2 + x + A$. *Sphinx* 6 (1936), 212 ~ 214.

1938 Skolem, T. *Diophantische Gleichungen.* Springer-Verlag, Berlin, 1938.

1947 Mills, W. H. A prime-representing function. *Bull. Amer. Math. Soc.* 53 (1947), p. 604.

1951 Wright, E. M. A prime-representing function. *Amer. Math. Monthly* 58 (1951), 616 ~ 618.

1952 Heegner, K. Diophantische Analysis und Modulfunktionen. *Math. Zeits.* 56 (1952), 227 ~ 253.

1960 Putnam, H. An unsolvable problem in number theory. *J. Symb. Logic* 1960 (220 ~ 232).

1962 Cohn, H. *Advanced Number Theory.* J. Wiley and Sons, New York, 1962. Reprinted by Dover, New York, 1980.

1964 Willans, C. P. On formulae for the nth prime. *Math. Gazette* 48 (1964), 413 ~ 415.

1966 Baker, A. Linear forms in the logarithms of algebraic numbers. *Mathematika* 13 (1966), 204 ~ 216.

1967 Stark, H. M. A complete determination of the complex quadratic fields of class-number one. *Michigan Math. J.* 14 (1967), 1 ~ 27.

1968 Deuring, M. Imaginäre quadratische Zahlkörper mit der Klassenzahl Eins. *Invent. Math.* 5 (1968), 169 ~ 179.

1969 Dudley, U. History of a formula for primes. *Amer. Math. Monthly* 76 (1969), 23 ~ 28.

1969 Stark, H. M. A historical note on complex quadratic fields with class-number one. *Proc. Amer. Math. Soc.* 21 (1969), 254 ~ 255.

1971 Baker, A. Imaginary quadratic fields with class number 2. *Annals of Math.* (2) 94 (1971), 139 ~ 152.

1971 Baker, A. On the class number of imaginary quadratic fields. *Bull. Amer. Math. Soc.* 77 (1971), 678 ~ 684.

1971 Gandhi, J. M. Formulae for the nth prime. *Proc. Washington State Univ. Conf. on Number Theory,* 96 ~ 106. Pullman, WA, 1971.

1971 Matijasevič, Yu. V. Diophantine representation of the set of prime numbers. (in Russian). *Dokl. Akad. Nauk SSSR* 196 (1971), 770 ~ 773. English translation by R. N. Goss, *Soviet Math. Dokl.* 12 (1971), 354 ~ 358

1971 Stark, H. M. A transcendence theorem for class-number problems. *Annals of Math.* (2) 94 (1971), 153 ~ 173.

1972 Vanden Eynden, C. A proof of Gandhi's formula for the nth prime. *Amer. Math. Monthly* 79 (1972), p. 625.

1973 Davis, M. Hilbert's tenth problem is unsolvable. *Amer. Math. Monthly* 80 (1973), 233 ~ 269.

1973 Karst, E. New quadratic forms with high density of primes. *Elem. Math.* 28 (1973), 116 ~ 118.

1973 Weinberger, P. J. Exponents of the class groups of complex quadratic fields. *Acta Arith.* 22 (1973), 117 ~ 124.

1974 Golomb, S. W. A direct interpretation of Gandhi's formula. *Amer. Math. Monthly* 81 (1974), 752 ~ 754.

1974 Hendy, M. D. Prime quadratics associated with complex quadratic fields of class number two. *Proc. Amer. Math. Soc.* 43 (1974), 253 ~ 260.

1974 Szekeres, G. On the number of divisors of $x^2 + x + A$. *J. Number Theory* 6 (1974), 434 ~ 442.

1975 Ernvall, R. A formula for the least prime graeter than a given integer. *Elem. Math.* 30 (1975), 13 ~ 14.

1975 Jones, J. P. Diophantine representation of the Fibonacci numbers. *Fibonacci Quart.* 13 (1975), 84 ~ 88.

1975 Matijasevič, Yu. & Robinson, J. Reduction of an arbitrary diophantine equation to one in 13 unknowns. *Acta Arith.* 27 (1975), 521 ~ 553.

1976 Jones, J. P. , Sato, D. , Wada, H. & Wiens, D. Diophantine

representation of the set of prime numbers. *Amer. Math. Monthly* 83 (1976), 449 ~ 464.

1977 Goldfeld, D. M. The conjectures of Birch and Swinnerton-Dyer and the class numbers of quadratic fields. *Astérisque* 41/42 (1977), 219 ~ 227.

1977 Matijasevič, Yu. V. Primes are nonnegative values of a polynomial in 10 variables. *Zapiski Sem. Leningrad Mat. Inst. Steklov* 68 (1977), 62 ~ 82. English translation by L. Guy and J. P. Jones, *J. Soviet Math.* 15 (1981), 33 ~ 44.

1979 Jones, J. P. Diophantine representation of Mersenne and Fermat primes. *Acta Arith.* 35 (1979), 209 ~ 221.

1981 Ayoub, R. G. & Chowla, S. On Euler's polynomial. *J. Number Theory* 13 (1981), 443 ~ 445.

1983 Gross, B. & Zagier, D. Points de Heegner et dérivées de fonctions L. *C. R. Acad. Sci. Paris* 297 (1983), 85 ~ 87.

1986 Gross, B. H. & Zagier, D. B. Heegner points and derivatives of L-series. *Invent. Math.* 84 (1986), 225 ~ 320.

1986 Sasaki, R. On a lower bound for the class number of an imaginary quadratic field. *Proc. Japan Acad.* A (Math. Sci.) 62 (1986), 37 ~ 39.

1986 Sasaki, R. A characterization of certain real quadratic fields. *Proc. Japan Acad.* A (Math. Sci.) 62 (1986), 97 ~ 100.

1988 Ribenboim, P. Euler's famous prime generating polynomial and the class number of imaginary quadratic fields. *L'Enseign. Math.* 34 (1988), 23 ~ 42.

1989 Flath, D. E. *Introduction to Number Theory.* Wiley-Intersience, New York, 1989.

1989 Goetgheluck, P. On cubic polynomials giving many primes. *Elem. Math.* 44 (1989), 70 ~ 73.

1990 Louboutin, S. Prime producing quadratic polynomials and class-numbers of real quad- ratic fields, and Addendum. *Can. J. Math.* 42 (1990), 315 ~ 341 and p. 1131.

1991 Louboutin, S. Extensions du théorème de Frobenius-Rabinovisch. *C. R. Acad. Sci. Paris* 312 (1991), 711 ~ 714.

1995 Boston, N. , & Greenwood, M. L. Quadratics representing primes. *Amer. Math. Monthly* 102 (1995), 595 ~ 599.

1995 Lukes, R. F. , Patterson, C. D. & Williams, H. C. Numerical sieving devices: Their history and applications. *Nieuw Arch. Wisk.* (4) 13 (1995), 113 ~ 139.

1996 Mollin, R. A. *Quadratics.* CRC Press, Boca Raton, FL, 1996.

1996 Mollin, R. A. An elementary proof of the Rabinowitsch-Mollin-Williams criterion for real quadratic fields. *J. Math. Sci.* 7 (1996), 17 ~ 27.

1997 Mollin, R. A. Prime-producing quadratics. *Amer. Math. Monthly* 104 (1997), 529 ~ 544.

2000 Ribenboim, P. *My Numbers, My Friends.* Springer-Verlag, New York, 2000.

2003 Dress, F. & Landreau, B. Polynômes prenant beaucoup de valeurs premières. Prepringt, 2003.

2003 Jacobson, Jr. , M. J. & Williams, H. C. New quadratic polynomials with high densities of prime values. *Math. Comp.* 72 (2003), 499 ~ 519.

第四章参考文献

1849 de polignac, A. Recherches nouvelles sur les nombres premiers. *C. R. Acad. Sci. Paris* 29 (1849), 397 ~ 401; Rectification: 738 ~ 739.

1885 Meissel E. D. F. Berechnung der Menge von Primzahlen, welche innerhalb der ersten Milliarde natürlicher Zahlen vorkommen. *Math. Ann.* 25 (1885), 251 ~ 257.

1892 Sylvester, J. J. On arithmetical series. *Messenger of Math.* 21 (1892), 1~19 and 87~120. Reprinted in *Gesammelte Abhandlungen*, Vol. III, 573~587. Springer-Verlag, New York, 1968.

1901 von Koch, H. Sur la distribution des nombres premiers. *Acta Math.* 24 (1901), 159~182.

1901 Torelli, G. Sulla totalità dei numeri primi fino ad un limite assegnato. *Atti Reale Accad. Sci. Fis. Mat. Napoli* (2) 11 (1901), 1~222.

1901 Wolfskehl, P. Über eine Aufgabe der elementaren Arithmetik. *Math. Ann.* 54 (1901), 503~504.

1903 Gram, J. -P. Note sur les zéros de la fonction $\zeta(s)$ de Riemann. *Acta Math.* 27 (1903), 289~304.

1909 Landau, E. *Handbuch der Lehre von der Verteilung der Primzahlen.* Teubner, Leipzig, 1909. Reprinted by Chelsea, Bronx, NY, 1974.

1909 Lehmer, D. N. *Factor Table for the First Ten Millions.* Carnegie Inst. , Publication #105, Washington, 1909. Reprinted by Hafner, New York,1956.

1914 Lehmer, D. N. *List of Prime Numbers from 1 to 10,006,721.* Carnegie Inst. , Publication #165, Washington, 1914. Reprinted by Hafner, New

York, 1956.

1914 Littlewood, J. E. Sur la distribution des nombres premiers. *C. R. Acad. Sci. Paris* 158 (1914), 1869~1872.

1919 Brun, V. Le crible d'Eratosthène et le théorème de Goldbach. *C. R. Acad. Sci. Paris* 168 (1919), 544~546.

1919 Brun, V. La série $\frac{1}{5}+\frac{1}{7}+\frac{1}{11}+\frac{1}{13}+\frac{1}{17}+\frac{1}{19}+\frac{1}{29}+\frac{1}{31}+\frac{1}{41}+\frac{1}{43}+\frac{1}{59}+\frac{1}{61}+\cdots$ où les dénominateurs sont " nombres premiers jumeaux " est convergente ou finie. *Bull. Sci. Math.* (2) 43 (1919), 100~104 and 124~128.

1919 Ramanujan, S. A proof of Bertrand's postulate. *J. Indian Math. Soc.* 11 (1919), 181~182. Reprinted in *Collected Papers of Srinivasa Ramanujan* (edited by G. H. Hardy and P. V. Seshu Aiyar), 208~209. Cambridge Univ. Press, Cambridge, 1927. Reprinted by Chelsea, Bronx, NY, 1962.

1920 Brun, V. Le crible d'Eratosthène et le théorème de Goldbach. *Videnskapsselskapets Skrifter Kristiania, Mat. -nat. Kl.* , 1920, No. 3, 36 pages.

1923 Hardy, G. H. & Littlewood, J. E. Some problems of " Partitio Numerorum ", III: On the expression of a number as a sum of primes. *Acta Math.* 44 (1923), 1~70. Reprinted in *Collected Papers of G. H. Hardy*, Vol. I, 561~630. Clarendon Press, Oxford, 1966.

1930 Hoheisel, G. Primzahlprobleme in der Analysis. *Sitzungsberichte Berliner Akad. d. Wiss.* , 1930, 580~588.

1930 Schnirelmann, L. Über additive Eigenschaften von Zahlen. *Ann. Inst. Polytechn. Novočerkask,* 14, 1930, 3~28 and *Math. Ann.* 107 (1933), 646~690.

1931 Westzynthius, E. Über die Verteilung der Zahlen, die zu den n ersten Primzahlen teilerfremd sind. *Comm. Phys. Math. Hesingfors* (5) 25 (1931), 1~37.

1932 Erdös, P. Beweis eines Satzes von Tschebyscheff. *Acta Sci. Math. Szeged* 5 (1932), 194~198.

1933 Skewes, S. On the difference $\pi(x)-\mathrm{li}(x)$. *J. London Math. Soc.* 8 (1933), 277~283.

1934 Ishikawa, H. Über die Verteilung der Primzahlen. *Sci. Rep. Tokyo Bunrika Daigaku.* (A) 2 (1934), 27~40.

1934 Romanoff, N. P. Über einige Stätze der additiven Zahlentheorie. *Math. Ann.* 109 (1934), 668~678.

1935 Erdös, P. On the difference of consecutive primes. *Quart. J. Pure*

and Appl. Math. , Oxford, (2) 6 (1935), 124~128.

1936 Tschudakoff, N. G. On the zeros of Dirichlet's L-functions (in Russian). *Mat. Sbornik* 1 (1936), 591~602.

1937 Cramér, H. On the order of magnitude of the difference between consecutive prime numbers. *Acta Arith.* 2 (1937), 23~46.

1937 Ingham, A. E. On the difference between consecutive primes. *Quart. J. Pure and Appl. Math.* , Oxford, (2) 8 (1937), 255~266.

1937 Landau, E. *Über einige neuere Fortschritte der additiven Zahlentheorie.* Cambridge Univ. Press, Cambridge, 1937. Reprinted by Stechert-Hafner, New York,1964.

1937 van der Corput, J. G. Sur l'hypothèse de Goldbach pour presque tous les nombres pairs. *Acta Arith.* 2 (1937), 266~290.

1937 Vinogradov, I. M. Representation of an odd number as the sum of three primes (in Russian). *Dokl. Akad. Nauk SSSR* 15 (1937), 169~172.

1938 Estermann, T. Proof that almost all even positive integers are sums of two primes. *Proc. London Math. Soc.* 44 (1938), 307~314.

1938 Poulet, P. Table des nombres composés vérifiant le théorème de Fermat pour le module 2, jusqu' à 100.000.000. *Sphinx* 8 (1938), 42~52. Corrections: *Math. Comp.* 25 (1971), 944~945, and 26 (1972), p. 814.

1938 Rankin, R. A. The difference between consecutive prime numbers. *J. London Math. Soc.* 13 (1938), 242~247.

1938 Rosser, J. B. The nth prime is greater than $n \log n$. *Proc. London Math. Soc.* 45 (1938), 21~44.

1938 Tschudakoff, N. G. On the density of the set of even integers which are not representable as a sum of two odd primes (in Russian). *Izv. Akad. Nauk SSSR,* Ser. Mat. , 1 (1938), 25~40.

1939 van der Corput, J. G. Über summen von Primzahlen und Primzahlquadraten. *Math. Ann.* 116 (1939), 1~50.

1940 Erdös, P. The difference of consecutive primes. *Duke Math. J.* 6 (1940), 438~441.

1944 Chowla, S. There exists an infinity of 3-combinations of primes in A. P. *Proc. Lahore Phil. Soc.* 6 (1944), 15~16.

1944 Linnik, Yu. V. On the least prime in an arithmetic progression I. The basic theorem (in Russian). *Mat. Sbornik* 15 (57), (1944), 139~178.

1946 Brauer, A. On the exact number of primes below a given limit. *Amer. Math. Monthly* 9 (1946), 521~523.

1947 Khinchin, A. Ya. *Three pearls of Number Theory.* Original Russian

edition in OGIZ, Moscow, 1947. Translation into English published by Graylock Press, Baltimore, 1952.

1947 Rényi, A. On the representation of even numbers as the sum of a prime and an almost prime. *Dokl. Akad. Nauk SSSR* 56 (1947), 455~458.

1949 Clement, P. A. Congruences for sets of primes. *Amer. Math. Monthly* 56 (1949), 23~25.

1949 Erdös, P. On a new method in elementary number theory which leads to an elementary proof of the prime number theorem. *Proc. Nat. Acad. Sci. USA* 35 (1949), 374~384.

1949 Erdös, P. On the converse of Fermat's theorem. *Amer. Math. Monthly* 56 (1949), 623~624.

1949 Moser, L. A theorem on the distribution of primes. *Amer. Math. Monthly* 56 (1949), 624~625.

1949 Richert, H. E. Über Zerfällungen in ungleiche Primzahlen. *Math. Zeits.* 52 (1949), 342~343.

1949 Selberg, A. An elementary proof of Dirichlet's theorem about primes in an arithmetic progression. *Annals of Math.* 50 (1949), 297~304.

1949 Selberg, A. An elementary proof of the prime number theorem. *Annals of Math.* 50 (1949), 305~313.

1950 Erdös P. On almost primes. *Amer. Math. Monthly* 57 (1950), 404~407.

1950 Erdös, P. On integers of the form $2^k + p$ and some related problems. *Summa Bras. Math.* 2 (1950), 113~123.

1950 Hasse, H. *Vorlesungen über Zahlentheorie.* Springer-Verlag, Berlin, 1950.

1950 Selberg, A. An elementary proof of the prime number theorem for arithmetic progressions. *Can. J. Math.* 2 (1950), 66~78.

1951 Titchmarsh, E. C. *The Theory of the Riemann Zeta Function.* Clarendon Press, Oxford, 1951.

1956 Borodzkin, K. G. On the problem of I. M. Vinogradov's constant (in Russian). *Proc. Third Math. Congress, Moscow,* 1 (1956), p. 3.

1956 Erdös P. On pseudo-primes and Carmichael numbers. *Publ. Math. Debrecen.* 4 (1956), 201~206.

1957 Leech, J. Note on the distribution of prime numbers. *J. London Math. Soc.* 32 (1957), 56~58.

1957 Pan, C. D. On the least prime in an arithmetic progression. *Sci. Record (N. S.)* 1 (1957), 311~313.

1958 Pan, C. D. On the least prime in an arithmetic progression. *Acta Sci. Natur. Univ. Pekinensis* 4 (1958), 1~34.

1958 Schinzel, A. & Sierpiński, W. Sur certaines hypothèses concernant les nombres premiers. *Acta Arith.* 4 (1958), 185~208; Erratum, 5 (1959), p. 259.

1959 Killgrove, R. B. & Ralston, K. E. On a conjecture concerning the primes. *Math. Comp.* 13 (1959), 121~122.

1959 Lehmer, D. H. On the exact number of primes less than a given limit. *Illinois J. Math.* 3 (1959), 381~388. Reprinted in *Selected Papers* (edited by D. McCarthy), Vol. III, 1104~1111. Ch. Babbage Res. Centre, St. Pierre, Manitoba, Canada, 1981.

1959 Schinzel, A. Démonstration d'une conséquence de l'hypothèse de Goldbach. *Compositio Math.* 14 (1959), 74~76.

1960 Golomb, S. W. The twin prime constant. *Amer. Math. Monthly* 67 (1960), 767~769.

1961 Prachar, K. Über die kleinste Primzahl einer arithmetischen Reihe. *J. Reine Angew. Math.* 206 (1961), 3~4.

1961 Schinzel, A. Remarks on the paper " Sur certaines hypothèses concernant les nombres premiers ". *Acta Arith.* 7 (1961), 1~8.

1961 Wrench, Jr. , J. W. Evaluation of Artin's constant and the twin-prime constant. *Math. Comp.* 15 (1961), 396~398.

1962 Rosser, J. B. & Schoenfeld, L. Approximate formulas for some functions of prime numbers. *Illinois J. Math.* 6 (1962),64~94.

1962 Schinzel,A. Remark on a paper of K. Prachar " Über die kleinste Primzahl einer arithmetischen Reihe ". *J. Reine Angew. Math.* 210 (1962), 121~122.

1963 Ayoub, R. G. *An Introduction to the Theory of Numbers.* Amer. Math. Soc. , Providence, RI, 1963.

1963 Kanold, H. -J. Elementare Betrachtungen zur Primzahltheorie. *Arch. Math.* 14 (1963), 147~151.

1963 Rankin, R. A. The difference between consecutive prime numbers, V. *Proc. Edinburgh Math. Soc.* (2) 13 (1963), 331~332.

1963 Rotkiewicz, A. Sur les nombres pseudo-premiers de la forme $ax + b$. *C. R. Acad. Sci. Paris* 257 (1963), 2601~2604.

1963 Walfisz, A. Z. *Weylsche Exponentialsummen in der neueren Zahlentheorie.* VEB Deuscher Verlag d. Wiss. , Berlin, 1963.

1964 Grosswald, E. A proof of the prime number theorem. *Amer. Math.*

Monthly 71 (1964), 736～743.

1964 Shanks, D. On maximal gaps between successive primes. *Math. Comp.* 18 (1964), 646～651.

1965 Chen, J. R. On the least prime in an arithmetical progression. *Sci. Sinica* 14 (1965), 1868～1871.

1965 Gelfond, A. O. & Linnik, Yu. V. *Elementary Methods in Analytic Number Theory.* Translated by A. Feinstein, revised and edited by L. J. Mordell. Rand McNally, Chicago, 1965.

1965 Rotkiewicz, A. Les intervalles contenant les nombres pseudo-premiers. *Rend. Circ. Mat. Palermo* (2) 14 (1965), 278～280.

1965 Stein, M. L. & Stein, P. R. New experimental results on the Goldbach conjecture. *Math. Mag.* 38 (1965), 72～80.

1965 Stein, M. L. & Stein, P. R. Experimental result on additive 2-bases. *Math. Comp.* 19 (1965), 427～434.

1966 Bombieri, E. & Davenport, H. Small differences between prime numbers. *Proc. Roy. Soc.* (A) 293 (1966), 1～18.

1967 Lander, L. J. & Parkin, T. R. On first appearance of prime differences. *Math. Comp.* 21 (1967), 483～488.

1967 Lander, L. J. & Parkin, T. R. Consecutive primes in arithmetic progression. *Math. Comp.* 21 (1967), p. 489.

1967 Rotkiewicz, A. On the pseudo-primes of the form $ax + b$. *Proc. Cambridge Phil. Soc.* 63 (1967), 389～392.

1967 Szymiczek, K. On pseudoprimes which are products of distinct primes. *Amer. Math. Monthly* 74 (1967), 35～37.

1969 Montgomery, H. L. Zeros of L-function. *Invent. Math.* 8 (1969), 346～354.

1969 Rosser, J. B. , Yohe, J. M. & Schoenfeld, L. Rigorous computation of the zeros of the Riemann zeta-function (with discussion). *Inform. Processing* 68 (Proc. IFIP Congress, Edinburgh, 1968), Vol. I, 70～76. North-Holland, Amsterdam, 1969.

1970 Diamond, H. G. & Steinig, J. An elementary proof of the prime number theorem with a remainder term. *Invent. Math.* 11 (1970), 199～258.

1972 Huxley, M. N. On the difference between consecutive primes. *Invent. Math.* 15 (1972), 164～170.

1972 Huxley, M. N. *The Distribution of Prime Numbers.* Oxford Univ. Press, Oxford 1972.

1972 Rotkiewicz, A. On a problem of W. Sierpiński. *Elem. Math.* 27 (1972), 83~85.

1973 Brent, R. P. The first occurence of large gaps between successive primes. *Math. Comp.* 27 (1973), 959~963.

1973/1978 Chen J. R. On the representation of a large even integer as the sum of a prime and the product of at most two primes, I and II. *Sci. Sinica* 16 (1973), 157~176, and 21 (1978), 421~430.

1973 Montgomery, H. L. The pair correlation of zeros of the zeta function. *Analytic Number Theory* (Proc. Symp. Pure Math. , Vol. XXIV, St, Louis, 1972), 181~193. Amer. Math. Soc. , Providence, RI, 1973.

1973 Montgomery, H. L. & Vaughan, R. C. The large sieve. *Mathematika* 20 (1973), 119~134.

1974 Ayoub, R. G. Euler and the zeta-function. *Amer. Math. Monthly* 81 (1974), 1067~1086.

1974 Edwards, H. M. *Riemann's Zeta Function.* Academic Press, New York, 1974.

1974 Halberstam, H. & Richert, H. E. *Sieve Methods.* Academic Press, New York, 1974.

1974 Hensley, D. & Richards, I. Primes in intervals. *Acta Arith.* 25 (1974), 375~391.

1974 Levinson, N. More than one third of zeros of Riemann's zeta function are on $\sigma = 1/2$. *Adv. in Math.* 13 (1974), 383~436.

1974 Mąkowski, A. On a problem of Rotkiewicz on pseudoprimes. *Elem. Math.* 29 (1974), p. 13.

1974 Richards, I. On the incompatibility of two conjectures concerning primes; a discussion of the use of computers in attacking a theoretical problem. *Bull. Amer. Math. Soc.* 80 (1974), 419~438.

1974 Shanks, D. & Wrench, J. W. Brun's constant. *Math. Comp.* 28 (1974), 293~299.

1975 Brent, R. P. Irregularities in the distribution of primes and twin primes. *Math. Comp.* 29 (1975), 43~56.

1975 Montgomery, H. L. & Vaughan, R. C. The exceptional set in Goldbach's problem. *Acta Arith.* 27 (1975), 353~370.

1975 Ross, P. M. On Chen's theorem that each large even number has the form p_1+p_2 or $p_1+p_2p_3$. *J. London Math. Soc.* (2) 10 (1975), 500~506.

1975 Rosser, J. B. & Schoenfeld, L. Sharper bounds for the Chebyshev functions $\theta(x)$ and $\psi(x)$. *Math. Comp.* 29 (1975), 243~269.

1075 Swift, J. D. Table of Carmichael numbers to 10^9. *Math. Comp.* 29 (1975), 338~339.

1975 Udrescu, V. S. Some remarks concerning the conjecture $\pi(x+y) \leqslant \pi(x)+\pi(y)$. *Rev. Roumaine Math. Pures Appl.* 20 (1975), 1201~1209.

1976 Apostol, T. M. *Introduction to Analytic Number Theory.* Springer-Verlag, New York, 1976.

1976 Brent, R. P. Tables concerning irregularities in the distribution of primes and twin primes to 10^{11}. *Math. Comp.* 30 (1976), p. 379.

1977 Hudson, R. H. A formula for the exact number of primes below a given bound in any arithmetic progressions. *Bull. Austral. Math. Soc.* 16 (1977), 67~73.

1977 Hudson, R. H. & Brauer, A. On the exact number of primes in the arithmetic progression $4n \pm 1$ and $6n \pm 1$. *J. Reine Angew. Math.* 291 (1977), 23~29.

1977 Huxley, M. N. Small differences between consecutive primes, II. *Mathematika* 24 (1977), 142~152.

1977 Jutila, M. On Linnik's constant. *Math. Scand.* 41 (1977), 45~62.

1977 Langevin, M. Méthodcs élémentaires en vue du théorème de Sylvester. *Sém. Delange-Pisot-Poitou,* 17[e] année, 1975/76, fasc. 1, exp. No. G12, 9 pages, Paris, 1977.

1977 Weintraub, S. Seventeen prtimes in arithmetic progression. *Math. Comp.* 31 (1977), p. 1030.

1978 Bays, C. & Hudson, R. H. On the fluctuations of Littlewood for primes of the form $4n \pm 1$. *Math. Comp.* 32 (1978), 281~286.

1978 Heath-Brown, D. R. Almost-primes in arithmetic progressions and short intervals. *Math. Proc. Cambridge Phil. Soc.* 83 (1978), 357~375.

1979 Heath-Brown, D. R. & Iwaniec, H. On the difference between consecutive powers. *Bull. Amer. Math. Soc.* (N. S.) 1 (1979), 758~760.

1979 Iwaniec, H. & Jutila, M. Primes in short intervals. *Arkiv för Mat.* 17 (1979), 167~176.

1979 Pomerance, C. The prime number graph. *Math. Comp.* 33 (1979), 399~408.

1979 Ribenboim, P. *13 Lectures on Fermat's Last Theorem.* Springer-Verlag, New York, 1979.

1979 Wagstaff, Jr. , S. S. Greatest of the least primes in arithmetic progressions having a given modulus. *Math. Comp.* 33 (1979), 1073~1080.

1979 Yorinaga, M. Numerical computation of Carmichael numbers, II.

Math. J. Okayama Univ. 21 (1979), 183～205.

1980 Brent, R. P. The first occurrence of certain large prime gaps. *Math. Comp.* 35 (1980), 1435～1436.

1980 Chen, J. R. & Pan, C. D. The exceptional set of Goldbach numbers, I. *Sci. Sinica* 23 (1980), 416～430.

1980 Light, W. A. , Forrest, J. , Hammond, N. & Roe, S. A note on Goldbach's conjecture. *BIT* 20 (1980), p. 525.

1980 Newman, D. J. Simple analytic proof of the prime number theorem. *Amer. Math. Monthly* 87 (1980), 693～696.

1980 Pintz, J. On Legendre's prime number formula. *Amer. Math. Monthly* 87 (1980), 733～735.

1980 Pomerance, A. A note on the least prime in an arithmetic progression. *J. Number Theory* 12 (1980), 218～223.

1980 Pomerance, C. , Selfridge, J. L. & Wagstaff, Jr. , S. S. The pseudoprimes to $25 \cdot 10^9$. *Math. Comp.* 35 (1980), 1003～1026.

1980 van der Poorten, A. J. & Rotkiewicz, A. On strong pseudoprimes in arithmetic progressions. *J. Austral. Math. Soc.* (A) 29 (1980), 316～321.

1981 Graham, S. On Linnik's constant. *Acta Arith.* 39 (1981), 163～179.

1981 Heath-Brown, D. R. Three primes and an almost prime in arithmetic progression. *J. London Math. Soc.* (2) 23 (1981), 396～414.

1981 Pomerance, C. On the distribution of pseudoprimes. *Math. Comp.* 37 (1981), 587～593.

1982 Diamond, H. G. Elementary methods in the study of the distribution of prime numbers. *Bull. Amer. Math. Soc.* (N. S) 7 (1982), 553～589.

1982 Pomerance, C. A new lower bound for the pseudoprimes counting function. *Illinois, J. Math.* 26 (1982), 4～9.

1982 Pritchard, P. A. 18 primes in arithmetic progression. *J. Recr. Math.* 15 (1982/3), 288.

1982 Weintraub, S. A prime gap of 682 and a prime arithmetic sequence. *BIT* 22 (1982), 538.

1983 Chen J. R. The exceptional value of Goldbach numbers, II. *Sci. Sinica* (A) 26 (1983), 714～731.

1983 Powell, B. Problem 6429 (Difference between consecutive primes). *Amer. Math. Monthly* 90 (1983), 338.

1983 Riesel, H. & Vaughan, R. C. On sums of primes. *Arkiv för Mat.* 21 (1983), 45～74.

1983 Robin, G. Estimation de la fonction de Tschebychef θ sur le $k^{\text{ième}}$ nombre premier et grandes valeurs de la fonction $\omega(n)$, nombre de diviseurs premiers de n. *Acta Arith.* 42 (1983), 367～389.

1984 Daboussi, H. Sur le théorème des nombres premiers. *C. R. Acad. Sci. Paris* 298 (1984), 161～164.

1984 Davies, R. O. Solution of problem 6429. *Amer. Math. Monthly* 91 (1984), 64.

1984 Iwaniec, H. & Pintz, J. Primes in short intervals. *Monatsh. Math.* 98 (1984), 115～143.

1984 Schroeder, M. R. *Number Theory in Science and Communication.* Spr-inger-Verlag, New York, 1984.

1984 Wang Y. *Goldbach Conjecture.* World Scientific Publ. Singapore, 1984.

1985 Heath-Brown, D. R. The ternary Goldbach problem. *Rev. Mat. Iberoamer.* 1 (1985), 45～58.

1985 Ivić, A. *The Riemann Zeta-Function.* J. Wiley and Sons, New York, 1985.

1985 Lagarias, J. C. Miller, V. S. & Odlyzko, A. M. Computing $\pi(x)$: The Meissel-Lehmer method. *Math. Comp.* 44 (1985), 537～560.

1985 Lou, S. & Yao, Q. The upper bound of the difference between consecutive primes. *Kexue Tongbao* 8 (1985), 128～129.

1985 Maier, H. Primes in short intervals. *Michigan Math. J.* 32 (1985), 221～225.

1985 Odlyzko, A. M. & te Riele, H. J. J. Disproof of the Mertens conjecture. *J. Reine Angew. Math.* 357 (1985), 138～160.

1985 Powell, B. Problem 1207 (A generalized weakened Goldbach theorem). *Math. Mag.* 58 (1985), 46.

1985 Pritchard, P. A. Long arithmetic progressions of primes: some old, some new. *Math. Comp.* 45 (1985), 263～267.

1985 te Riele, H. J. J. Some historical and other notes about the Mertens conjecture and its recent disproof. *Nieuw Arch. Wisk.* (4) 3 (1985), 237～243.

1986 Bombieri, E. , Friedlander, J. B. & Iwaniec, H. Primes in arithmetic progression to large moduli, I. *Acta Maht.* 156 (1986), 203～251.

1986 Finn, M. V. & Frohliger, J. A. Solution of problem 1207. *Math. Mag.* 59 (1986), 48～49.

1986 Mozzochi, C. J. On the difference between consecutive primes. *J.*

Number Theory 24 (1986), 181~187.

1986 van de Lune, J. , te Riele, H. J. J. & Winter, D. T. On the zeros of the Riemann zeta function in the critical strip, IV. *Math. Comp.* 46 (1986), 667~681.

1986 Wagon, S. Where are the zeros of zeta of s?. *Math. Intelligencer* 8, No. 4 (1986), 57~62.

1987 Pintz, J. An effective disproof of the Mertens conjecture. *Astérisque* 147/148 (1987), 325~333.

1987 te Riele, H. J. J. On the sign of the difference $\pi(x) - \mathrm{li}(x)$. *Math. Comp.* 48 (1987), 323~328.

1988 Erdös, P. , Kiss, P. & Sárközy, A. A lower bound for the counting function of Lucas pseudoprimes. *Math. Comp.* 51 (1988), 315~323.

1988 Odlyzko, A. M. & Schönhage, A. Fast algorithms for multiple evaluations of the Riemann zeta function. *Trans. Math. Soc.* 309 (1988), 797~809.

1988 Patterson, S. J. *Introduction to the Theory of the Riemann Zeta-Function.* Cambridge Univ. Press, Cambridge, 1988.

1989 Chen, J. R & Liu, J. M. On the least prime in an arithmetical progression, III and IV. *Sci. China* (A) 32 (1989), 654~673 and 792~807.

1989 Chen, J. R & Wang, T. Z. On the odd Goldbach problem. *Acta Math. Sinica* 32 (1989), 702~718.

1989 Conrey, J. B. At least two fifths of the zeros of the Riemann zeta function are on the critical line. *Bull. Amer. Math. Soc.* 20 (1989), 79~81.

1989 Granville, A. , van de Lune, J. & te Riene, H. J. J. Checking the Goldbach conjecture on a vector computer. In *Number Theory and Applications.* (edited by R. A. Mollin). Kluwer, Dordrecht, 1989, 423~432

1989 Young, J & Potler, A. First occurrence of prime gaps. *Math. Comp.* 52 (1989), 221~224.

1990 Granville, A. & Pomerance, C. On the least prime in certain arithmetic progressions. *J. London Math. Soc.* (2) 41 (1990), 193~200.

1990 Jaeschke, G. The Carmichael numbers to 10^{12}. *Math. Comp.* 55 (1990), 383~389.

1990 Parady, B. K. , Smith, J. F. & Zarantonello, S. Largest known twin primes. *Math. Comp.* 55 (1990), 381~382.

1991 Weintraub, S. A prime gap of 784. *J. Recr. Math.* 23, No. 1 (1991), 6~7.

1992 Golomb, S. Problem 10208. *Amer. Math. Monthly* 99 (1992), 266.

1992 Granville, A. Primality testing and Carmichael numbers. *Notices Amer. Math. Soc.* 39 (1992), 696~700.

1992 Heath-Brown, D. R. Zero-free regions for Dirichlet L-functions and the least prime in an arithmetic progression. *Proc. London Math. Soc.* (3) 64 (1992), 265~338.

1992 Pinch, R. G. E. The pseudoprimes up to 10^{12}. Unpublished manuscript.

1993 Deshouillers, J. -M. , Granville, A. , Narkiewicz, W. & Pomerance, C. An upper bound in Goldbach's problem. *Math. Comp.* 61 (1993), 209~213.

1993 Lou, S. & Yao, Q. The number of primes in a short interval. *Hardy-Ramanujan J.* 16 (1993), 21~43.

1993 Odlyzko, A. Iterated absolute values of differences of consecutive primes. *Math. Comp.* 61 (1993), 373~380.

1993 Pinch, R. G. E. The Carmichael numbers up to 10^{15}. *Math. Comp.* 61 (1993), 381~391.

1993 Pomerance, C. Carmichael numbers. *Nieuw Arch. Wisk.* (4) 11 (1993), 199~209.

1993 Sinisalo, M. K. Checking the Goldbach conjecture up to 4×10^{11}. *Math. Comp.* 61 (1993), 931~934.

1994 Alford, W. R. , Granville, A. & Pomerance, C. There are infinitely many Carmichael numbers. *Annals of Math.* 140 (1994), 703~722.

1994 Lou, S. & Yao, Q. Estimates of sums of Dirichlet series. *Hardy-Ramanujan J.* 17 (1994), 1~31.

1995 Ford, K. Solution of problem 10208. *Amer. Math. Monthly* 102 (1995), 361~362.

1995 Nicely, T. R. Enumeration to 10^{14} of the twin primes and Brun's constant. *Virginia J. of Sci.* 46 (1995), 195~204.

1995 Pritchard, P. A. , Moran, A. & Thyssen, A. Twenty-two primes in arithmetic progression. *Math. Comp.* 64 (1995), 1337~1339.

1995 Ramaré, O. On Snirel'man's constant. *An. Scuola Norm. Sup. Pisa, Cl. Sci.* (4) 22 (1995), 645~706.

1996 Chen, J. R. & Wang, T. Z. The Goldbach problem for odd numbers. *Acta Math. Sinica* 39 (1996), 169~174.

1996 Connes, A. Formule de trace en géométrie non-commutative et hypothèse de Riemann. *C. R. Acad. Sci. Paris* 323 (1996), 1231~1236.

1996 Deléglise, M. & Rivat, J. Computing $\pi(x)$: The Meissel, Lehmer,

Lagarias, Miller, Odlyzko method. *Math. Comp.* 65 (1996), 235~245.

1996 Indlekofer, H. -J. & Járai, A. Largest known twin primes. *Math. Comp.* 65 (1996), 427~428.

1996 Massias, J. -P. & Robin, G. Bornes effectives pour certaines fonctions concernant les nombres premiers. *J. Théor. Nombres Bordeaux* 8 (1996), 215~242.

1996 Ramaré, O. & Rumely, R. Primes in arithmetic progressions. *Math. Comp.* 65 (1996), 397~425.

1996 Shiu, D. *Prime Numbers in Arithmetical Progressions.* Ph. D Thesis, Univ. of Oxford, 1996.

1997 Deshouillers, J. -M. , Effinger, G. , te Riele, H. & Zinoviev, D. A complete Vinogradov 3-primes theorem under the Riemann Hypothesis. *Electron. Res. Announc. Amer. Math. Soc.* 3 (1997), 99~104.

1997 Dubner, H. & Nelson, H. Seven Consecutive primes in arithmetic progression. *Math. Comp.* 66 (1997), 1743~1749.

1997 Forbes, T. A large pair of twin primes. *Math. Comp.* 66 (1997), 451~455.

1997 Mollin, R. A. Prime-producing quadratics. *Amer. Math. Monthly* 104 (1997), 529~544.

1998 Deléglise, M. & Rivat, J. Computing $\psi(x)$. *Math. Comp.* 67 (1998), 1691~1696.

1998 Deshoulliers, J. -M. , te Riele, H. J. J. & Saouter, Y. New experimental results concerning the Goldbach conjecture. In *Proc. Third Int. Symp. on Algorithmic Number Th.* (edited by J. P. Buhler). Lecture Notes in Computer Sci. #1423, 204~215. Springer-Verlag, New York, 1998

1998 Dusart, P. Autour de la fonction qui compte le nombre de nombres premiers. Ph. D. Thesis, Université de Limoges, 1998, 171 pages.

1998 Pinch, R. G. E. The Carmichael numbers up to 10^{16}. Unpublished manuscript.

1998 Saouter, Y. Checking the odd Goldbach conjecture up to 10^{20}. *Math. Comp.* 67 (1998), 863~866.

1999 Dusart, P. The kth prime is greater than $k(\ln k + \ln\ln k - 1)$ for $k \geqslant 2$. *Math. Comp.* 68 (1999), 411~415.

1999 Dusart, P. Intégalités explicites pour $\psi(x), \theta(x), \pi(x)$ et les nombres premiers. *C. R. Math. Rep. Acad. Sci. Canada* 21 (1999), 53~59.

1999 Forbes, T. Prime clusters and Cunningham chains. *Math. Comp.* 68 (1999), 1739~1747.

1999 Indlekofer, H. -J. & Járai, A. Largest known twin primes and Sophie Germain primes. *Math. Comp.* 68 (1999), 1317~1324.

1999 Nicely, T. R. New maximal prime gaps and first occurrences. *Math. Comp.* 68 (1999), 1311~1315.

1999 Nicely, T. R. Enumeration to 1.6×10^{15} of the prime quadruplets. Preprint, 1999.

1999 Nicely, T. R. & Nyman, B. First occurrence of a prime gap of 1000 or greater. Preprint, 1999.

2000 Bays, C. & Hudson, R. H. A new bound for the smallest x with $\pi(x) > \mathrm{li}(x)$. *Math. Comp.* 69 (2000), 1285~1296.

2000 Pinch, R. G. E. The pseudoprimes up to 10^{13}. In *Proc. Fourth Int. Symp. on Algorithmic Number Th.* (edited by W. Bosma). Lecture Notes in Computer Sci. #1838, 459~474. Springer-Verlag, New York, 2000.

2000 Shiu, D. K. L. Strings of congruent primes. *J. London Math. Soc.* (2) 61 (2000), 359~373.

2001 Baker, R. C. , Harman, G. & Pintz, J. The difference between consecutive primes, II. *Proc. London Math. Soc.* (3) 83 (2001), 532~562.

2001 Kadiri, H. Une région explicite sans zéros pour la fonction zeta de Riemann. Preprint, 2001.

2001 Nicely, T. R. A new error analysis for Brun's constant. *Virginia J. of Sci.* 52 (2001), 45~55.

2001 Odlyzko, A. M. The 10^{22}-nd zero of the Riemann zeta function. In *Dynamical, Spectral, and Arithmetic Zeta Functions.* (edited by M. L. Lapidus and M. van Frankenhuysen), 139~144. Contemporary Math. , Vol. 290, Amer. Math. Soc. , Providence, RI, 2001.

2001 Richstein, J. Verifying the Goldbach conjecture up to $4 \cdot 10^{14}$. *Math. Comp.* 70 (2001), 1745~1749.

2002 Dubner, H. , Forbes, T. , Lygeros, N. , Mizony, M. , Nelson, H. & Zimmermann, P. Ten consecutive primes in arithmetic progression. *Math. Comp.* 71 (2002), 1323~1328.

2002 Dusart, P. Sur la conjecture $\pi(x+y) \leqslant \pi(x) + \pi(y)$. *Acta Arith.* , 102 (2002), 295~308.

2003 Ramaré, O. & Saouter, Y. Short effective intervals containing primes. *J. Number Theory* 98 (2003), 10~33.

第五章参考文献

1948 Gunderson, N. G. *Derivation of Criteria for the First Case of Fer-*

mat's Last Theorem and the Combination of these Criteria to Produce a New Lower Bound for the Exponent. Ph. D. Thesis, Cornell University, 1948, 111 pages.

1951 Dénes, P. An extension of Legendre's criterion in connection with first case of Fermat's last theorem. *Publ. Math. Debrecen* 2 (1951), 115~120.

1953 Goldberg, K. A table of Wilson quotients and the third Wilson prime. *J. London Math. Soc.* 28 (1953), 252~256.

1954 Ward, M. Prime divisors of second order recurring sequences. *Duke Math. J.* 21 (1954), 607~614.

1956 Obláth, R. Une propriété des puissances parfaites. *Mathesis* 65 (1956), 356~364.

1956 Riesel, H. Några stora primtal. *Elementa* 39 (1956), 258~260.

1958 Jarden, D. *Recurring Sequences.* Riveon Lematematika, Jerusalem, 1958 (3rd edition, 1973).

1958 Robinson, R. M. A report on primes of form $k \cdot 2^n + 1$ and on factors of Fermat numbers. *Proc. Amer. Math. Soc.* 9 (1958), 673~681.

1960 Sierpiński, W. Sur un problème concernant les nombres $k \cdot 2^n + 1$. *Elem. Math.* 15 (1960), 73~74.

1964 Graham, R. L. A Fibonacci-like sequence of composite numbers. *Math. Mag.* 37 (1964), 322~324.

1964 Riesel, H. Note on the congruence $a^{p-1} \equiv 1 \pmod{p^2}$. *Math. Comp.* 18 (1964), 149~150.

1964 Siegel, C. L. Zu zwei Bemerkungen Kummers. *Nachr. Akad. d. Wiss. Göttingen, Math. Phys. Kl.* , II, 1964, 51~62. Reprinted in *Gesammelte Abhandlungen* (edited by K. Chandrasekharan and H. Maas), Vol. III, 436~442. Springer-Verlag, Berlin, 1966.

1965 Kloss, K. E. Some number theoretic calculations. *J. Res. Nat. Bureau of Stand.* B, 69 (1965), 335~336.

1966 Hasse, H. Über die Dichte der Primzahlen p, für die eine vorgegebene ganzrationale Zahl $a \neq 0$ von gerader bzw. ungerader Ordnung mod p ist. *Math. Ann.* 168 (1966), 19~23.

1966 Kruyswijk, D. *On the congruence $u^{p-1} \equiv 1 \pmod{p^2}$* (in Dutch). Math. Centrum Amsterdam, 1966, 7 pages.

1969 Riesel, H. Lucasian criteria for the primality of $N = h \cdot 2^n - 1$. *Math. Comp.* 23 (1969), 869~875.

1971 Brillhart, J. , Tonascia, J. & Weinberger, P. J. On the Fermat quotient. In *Computers in Number Theory.* (edited by A. L. Atkin and

B. J. Birch), 213~222. Academic Press, New York, 1971.

1975 Johnson, W. Irregular primes and cyclotomic invariants. *Math. Comp.* 29 (1975), 113~120.

1976 Hooley, C. *Application of Sieve Methods to the Theory of Numbers.* Cambridge Univ. Press, Cambridge, 1976.

1978 Wagstaff, Jr. , S. S. The irregular primes to 125000. *Math. Comp.* 32 (1978), 583~591.

1978 Williams, H. C. Some primes with interesting digit patterns. *Math. Comp.* 32 (1978), 1306~1310.

1979 Erdös, P. & Odlyzko, A. M. On the density of odd integers of the form $(p-1)2^{-n}$ and related questions. *J. Number Theory* 11 (1979), 257~263.

1979 Ribenboim, P. *13 Lectures on Fermat's Last Theorem.* Springer-Verlag, New York, 1979.

1979 Williams, H. C. & Seah, E. Some primes of the form $(a^n-1)/(a-1)$. *Math. Comp.* 33 (1979), 1337~1342.

1980 Newman, M. , Shanks, D. & Williams, H. C. Simple groups of square order and an interesting sequence of primes. *Acta Arith.* 38 (1980), 129~140.

1980 Powell, B. Primitive densities of certain sets of primes. *J. Number Theory* 12 (1980), 210~217.

1981 Lehmer, D. H. On Fermat's quotient, base two. *Math. Comp.* 36 (1981), 289~290.

1982 Powell, B. Problem E 2956 (The existence of small prime solutions of $x^{p-1} \not\equiv 1 (\mathrm{mod}\ p^2)$). *Amer. Math. Monthly* 89 (1982), 498.

1982 Yates, S. *Repunits and Repetends.* Star Publ. Co. , Boynton Beach, FL, 1982.

1983 Jaeschke, G. On the smallest k such that $k \cdot 2^N + 1$ are composite. *Math. Comp.* 40 (1983), 381~384; Corrigendum, 45 (1985), p. 637.

1983 Keller, W. Factors of Fermat numbers and large primes of the form $k \cdot 2^n + 1$. *Math. Comp.* 41 (1983), 661~673.

1983 Ribenboim, P. 1093. *Math. Intelligencer.* 5, No. 2 (1983), 28~34.

1985 Lagarias, J. C. The set of primes dividing the Lucas numbers has density $\frac{2}{3}$. *Pacific J. Math.* 118 (1985), 19~23.

1986 Tzanakis, N. Solution to problem E 2956. *Amer. Math. Monthly* 93 (1986), p. 569.

1986 Williams, H. C. & Dubner, H. The primality of R1031. *Math.*

Comp. 47 (1986), 703~711.

1987 Granville, A. *Diophantine Equations with Variable Exponents with Special Reference to Fermat's Last Theorem.* Ph. D. Thesis, Queen's University, Kingston, 1987, 207 pages.

1987 Rotkiewicz, A. Note on the diophantine equation $1+x+x^2+\cdots+x^n = y^m$. *Elem. Math.* 42 (1987), p. 76.

1988 Brillhart, J. , Montgomery, P. L. & Silverman, R. D. Tables of Fibonacci and Lucas factorizations, and Supplement. *Math. Comp.* 50 (1988), 251~260, S1-S15.

1988 Gonter, R. H. & Kundert, E. G. *Wilson's theorem* $(n-1)! \equiv -1 \pmod{p^2}$ *has been computed up to* 10,000,000. Fourth SIAM Conference on Discrete Mathematics, San Francisco, June 1988.

1988 Granville, A. & Monagan, M. B. The first case of Fermat's last theorem is true for all prime exponents up to 714,591,416,091,389. *Trans. Amer. Math. Soc.* 306 (1988), 329~259.

1989 Dubner, H. Generalized Cullen Numbers. *J. Recr. Math.* 21 (1989), 190~194.

1989 Löh, G. Long chain of nearly doubled primes. *Math. Comp.* 53 (1989), 751~759.

1989 Tanner, J. W. & Wagstaff, Jr. , S. S. New bound for the first case of Fermat's last theorem. *Math. Comp.* 53 (1989), 743~750.

1990 Brown, J. , Noll, L. C. , Parady, B. K. , Smith, J. F. , Smith, G. W. & Zarantonello, S. Letter to the editor. *Amer. Math. Monthly* 97 (1990), p. 214.

1990 Knuth, D. A Fibonacci-like sequence of composite numbers. *Math. Mag.* 63 (1990), 21~25.

1991 Aaltonen, M. & Inkeri, K. Catalan's equation $x^p - y^p = 1$ and related congruences. *Math. Comp.* 56 (1991), 359~370. Reprinted in *Collected Papers of Kustaa Inkeri* (edited by T. Metsänkylä and P. Ribenboim), Queen's Papers in Pure and Appl. Math. 91, 1992, Queen's Univ. Kingston, Ontario, Canada.

1991 Fee, G & Granville, A. The prime factors of Wendt's binomial circulant determinant. *Math. Comp.* 57 (1991), 839~848.

1991 Keller, W. Woher kommen die größten derzeit bekannten Primzahlen? *Mitt. Math. Ges. Hamburg* 12 (1991), 211~229.

1992 Buhler, J. P. , Crandall, R. E. & Sompolski, R. W. Irregular primes to one million. *Math. Comp.* 59 (1992), 717~722.

1993 Buhler, J. P. , Crandall, R. E. , Ernvall, R. & Metsänkylä, T. Irregular primes and cyclotomic invariants to four million. *Math. Comp.* 61 (1993), 151~153.

1993 Dubner, H. Generalized repunit primes. *Math. Comp.* 61 (1993), 927~930.

1993 Montgomery, P. L. New solutions of $a^{p-1} \equiv 1 \pmod{p^2}$. *Math. Comp.* 61 (1993), 361~363.

1994 Crandall, R. & Fagin, B. Discrete weighted transforms and large-integer arithmetic. *Math. Comp.* 62 (1994), 305~324.

1994 Gonter, R. H. & Kundert, E. G. *All prime numbers up to 18,876,041 have been tested without finding a new Wilson prime.* Unpublished manuscript, Amberst, MA, 1994, 10 pages.

1994 Suzuki, J. On the generalized Wieferich criteria. *Proc. Japan Acad. Sci.* A (Math. Sci.), 70 (1994), 230~234.

1995 Keller, W. New Cullen primes. *Math. Comp.* 64 (1995), 1733~1741.

1995 Keller, W. & Niebuhr, W. Supplement to "New Cullen primes". *Math. Comp.* 64 (1995), S39~S46.

1997 Crandall, R. , Dilcher, K. & Pomerance, C. A search for Wieferich and Wilson primes. *Math. Comp.* 66 (1997), 433~449.

1997 Ernvall, R. & Metsänkylä, T. On the p-divisibility of Fermat quotients. *Math. Comp.* 66 (1997), 1353~1365.

1999 Dubner, H. & Keller, W. New Fibonacci and Lucas primes. *Math. Comp.* 68 (1999), 417~427, S1~S12.

1999 Forbes, T. Prime clusters and Cunningham chains. *Math. Comp.* 68 (1999), 1739~1747.

1999 Ribenboim, P. *Fermat's Last Theorem for Amateurs.* Springer-Verlag, New York, 1999.

2000 Pinch, R. G. E. The pseudoprimes up to 10^{13}. In *Proc. Fourth Int. Symp. on Algorithmic Number Th.* (edited by W. Bosma). Lecture Notes in Computer Sci. #1838, 459~474. Springer-Verlag, New York, 2000.

2001 Buhler, J. , Crandall, R. , Ernvall, R. , Metsänkylä, T. & Shokrollahi, M. A. Irregular primes and cyclotomic invariants to 12 million. *J. Symbolic Comp.* 31 (2001), 89~96.

2001 Keller, W. & Richstein, J. Solutions of the congruence $a^{p-1} \equiv 1 \ (mod\ p^r)$. Preprint, 2001.

2002 Dubner, H. Repunit R49081 is a probable prime. *Math. Comp.* 71 (2002), 833~835.

2002 Dubner, H. & Gallot, Y. Distribution of generalized Fermat prime numbers. *Math. Comp.* 71 (2002), 825～832.

2002 Izotov, A. S. Second-order linear recurrences of composite numbers. *Fibonacci Quart.* 40 (2002), 266～268.

2002 Sellers, J. A. & Williams, H. C. On the infinitude of composite NSW numbers. *Fibonacci Quart.* 40 (2002), 253～254.

2003 Knauer, J. & Richstein, J. The continuing search for Wieferich primes. Preprint, 2003.

第六章参考文献

1857 Bouniakowsky, V. Nouveaux théorèmes relatifs à la distribution des nombres premiers et à la décomposition des entiers en facteurs. *Mém. Acad. Sci. St. Petersbourg* (6), *Sci. Math. Phys.* , 6 (1857), 305～329.

1904 Dickson, L. E. A new extension of Dirichlet's theorem on prime numbers. *Messenger of Math.* 33 (1904), 155～161.

1922 Nagell, T. Zur Arithmetik der Polynome. *Abhandl. Math. Sem. Univ. Hamburg* 1 (1922), 179～194.

1923 Hardy, G. H. & Littlewood, J. E. Some problems in " Partitio Numerorum ", III: On the expression of a number as a sum of primes. *Acta Math.* 44 (1923), 1～70. Reprinted in *Collected Papers of G. H. Hardy*, Vol. I, 561～630. Clarendon Press, Oxford, 1966.

1931 Heilbronn, H. Über die Verteilung der Primzahlen in Polynomen. *Math. Ann.* 104 (1931), 794～799.

1932 Breusch, R. Zur Verallgemeinerung des Bertrandschen Postulates, dass zwischen x und $2x$ stets Primzahlen liegen. *Math. Zeits.* 34 (1932), 505～526.

1939 Beeger, N. G. W. H. Report on some calculations of prime numbers. *Nieuw Arch. Wisk.* 20 (1939), 48～50.

1958 Schinzel, A. & Sierpiński, W. Sur certaines hypothèses concernant les nombres premiers. Remarque. *Acta Arith.* 4 (1958), 185～208 and 5 (1959), p. 259.

1961 Schinzel, A. Remarks on the paper "Sur certaines hypothèses concernant les nombres premiers". *Acta Arith.* 7 (1961), 1～8.

1964 Sierpiński, W. Les binômes $x^2 + n$ et les nombres premiers. *Bull. Soc. Roy. Sci. Liège* 33 (1964), 259～260.

1969 Rieger, G. J. On polynomials and almost-primes. *Bull. Amer. Math. Soc.* 75 (1969), 100～103.

1971 Shanks, D. A low density of primes. *J. Recr. Math.* 4 (1971/2), 272～275.

1973 Wunderlich, M. C. On the Gaussian primes on the line $\text{Im}(x) = 1$. *Math. Comp.* 27 (1973), 399～400.

1974 Halberstam, H. & Richert, H. E. *Sieve Methods.* Academic Press, New York, 1974.

1975 Shanks, D. Calculation and application of Epstein zeta functions. *Math. Comp.* 29 (1975), 271～287.

1978 Iwaniec, H. Almost-primes represented by quadratic polynomials. *Invent. Math.* 47 (1978), 171～188.

1982 Powell, B. Problem 6384 (Numbers of the form $m^p - n$). *Amer. Math. Monthly* 89 (1982), p. 278.

1983 Israel, R. B. Solution of problem 6384. *Amer. Math. Monthly* 90 (1983), p. 650.

1984 Gupta, R. & Ram Murty, P. M. A remark on Artin's conjecture. *Invent. Math.* 78 (1984), 127～130.

1984 McCurley, K. S. Prime values of polynomials and irreducibility testing. *Bull. Amer. Math. Soc.* 11 (1984), 155～158.

1986 Heath-Brown, D. R. Artin's conjecture for primitive roots. *Quart. J. Math. Oxford* (2) 37 (1986), 27～38.

1986 McCurley, K. S. The smallest prime value of $x^n + a$. *Can. J. Math.* 38 (1986), 925～936.

1986 McCurley, K. S. Polynomials with no small prime values. *Proc. Amer. Math. Soc.* 97 (1986), 393～395.

1990 Fung, G. W. & Williams, H. C. Quadratic polynomials which have a high density of prime values. *Math. Comp.* 55 (1990), 345～353.

1994 Alford, W. R. , Granville, A. & Pomerance, C. There are infinitely many Carmichael numbers. *Annals of Math.* (2) 140 (1994), 703～722.

1995 Jacobson, Jr. , M. J. *Computational Techniques in Quadratic Fields.* M. A. Thesis, University of Manitoba, Winnipeg, 1995.

1998 Friedlander, J. & Iwaniec, H. The polynomial $x^2 + y^4$ captures its primes. *Annals of Math.* (2) 148 (1998), 945～1040.

2001 Dubner, H. & Forbes, T. Prime Pythagorean triangles. *J. Integer Seq.* 4 (2001), Art. 01. 2. 3, 1～11(electronic).

2001 Heath-Brown, D. R. Primes represented by $x^3 + 2y^3$. *Acta Math.* 186 (2001), 1～84.

2003 Jacobson, Jr. , M. J. & Williams, H. C. New quadratic polynomials

with high densities of prime values. *Math. Comp.* 72 (2003), 499~519.

附录 1

1935 Hall, P. On representative of subsets. *J. London Math. Soc.* 10 (1935), 26~30.

1969 Grimm, C. A. A Conjecture on consecutive composite numbers. *Amer. Math. Monthly* 76 (1969), 1126~1128.

1971 Erdös, P. & Selfridge, J. L. Some problems on the prime factors of consecutive integers, II. *Proc. Washington State Univ. Conf. on Number Theory.* (edited by J. H. Jordan and W. A. Webb), 13~21. Pullman, WA, 1971.

1975 Ramachandra, K. , Shorey, T. N. & Tijdeman, R. On Grimm's problem relating to factorisation of a block of consecutive integers. *J. Reine Angew. Math.* 273 (1975), 109~124.

附录 2

1981 Bateman, P. T. Major figures in the history of the prime number theorem. *Abstracts Amer. Math. Soc.* 2 (1981), 87th Annual Meeting, San Francisco, p. 2



一般性资源

Caldwell, C. The Prime Pages.Prime number research,records,and resources.

http://www.utm.edu/rasearch/primes

Weisstein,E. The World of Mathematics.Number theory.

http://mathworld.wolfram.com/topics/NumberTheory.html

与第二章有关的资源

Keller,W. Prime factors $k \cdot 2^n + 1$ of Fermat numbers F_m and complete factoring status.

http://www.prothsearch.net/fermat.html

Caldwell,C. the largest known Mersenne primes.

http://www.utm.edu/research/primes/largest.html#Mersenne

Woltman,G. Status of Great Internet Mersenne Prime Search.

http://www.mersenne.org/status.htm

Martin,M. Largest primes verified with the ECPP algorithm.

http://www.ellipsa.net/primes/top20.html

Kelly,B. Fibonacci and Lucas factorizations.

http://home.att.net/~blair.kelly/mathematics/fibonacci/

与第四章有关的资源

Gourdon,X.& Sebah,P. Counting the number of primes.

http://numbers.computation.free.fr/Constants/Primes
/countingPrimes.html

Wedeniwski,S. Verification of the Riemann hypothesis.

http://www.zetagrid.net/zeta/rh.html

Nicely,T.R. First occurrence prime gaps.

http://www.trnively.net/gaps/gaplist.html

Nicely,T.R. Counts of twin prime pairs.

http://www.trnicely.net/counts.html

Caldwell,C. The largest known twin primes.

http://www.utm.edu/research/primes/largest.html#twin

Forbes,T. Prime k-tuplets.

http://www.ltkz.demon.co.uk/ktuplets.htm

Oliveira e Silva,T. Goldbach conjecture verification.

http://www.ieeta.pt/tos/goldbach.html

与第五章有关的资源

Caldwell,C. The largest known Sophie Germain primes.
http://www.utm.edu/research/primes/largest.html#Sophie

Keller,W & Richstein,J. Fermat quotients $q_p(a)$ that are divisible by p.
http://www.informatik.uni-giessen.de/staff/richstein/cnth/FermatQuotient.html

Helm,L.& Norris,D. A distributed attack on the Sierpinski problem.
http://www.seventeenorbust.com/

Ballinger,R.& Keller,W. The Riesel problem:Definition and status.
http://www.prothsearch.net/rieselprob.html

Caldwell,C. The largest known (non-Mersenne) primes.
http://primes.utm.edu/primes/lists/all.txt

Leyland,P. Factorization of Cullen and Woodall numbers.
http://research.microsoft.com/~pleyland/factorization/cullen_woodall/cw.htm

Löh,G. Generalized Cullen primes.
http://www.rrz.uni-hamburg.de/RRZ/G.Loeh/gc/status.html



10 000 以内的素数

2	3	5	7	11	13	17	19	23	29
31	37	41	43	47	53	59	61	67	71
73	79	83	89	97	101	103	107	109	113
127	131	137	139	149	151	157	163	167	173
179	181	191	193	197	199	211	223	227	229
233	239	241	251	257	263	269	271	277	281
283	293	307	311	313	317	331	337	347	349
353	359	367	373	379	383	389	397	401	409
419	421	431	433	439	443	449	457	461	463
467	479	487	491	499	503	509	521	523	541
547	557	563	569	571	577	587	593	599	601
607	613	617	619	631	641	643	647	653	659
661	673	677	683	691	701	709	719	727	733
739	743	751	757	761	769	773	787	797	809
811	821	823	827	829	839	853	857	859	863
877	881	883	887	907	911	919	929	937	941
947	953	967	971	977	983	991	997	1009	1013
1019	1021	1031	1033	1039	1049	1051	1061	1063	1069
1087	1091	1093	1097	1103	1109	1117	1123	1129	1151
1153	1163	1171	1181	1187	1193	1201	1213	1217	1223
1229	1231	1237	1249	1259	1277	1279	1283	1289	1291
1297	1301	1303	1307	1319	1321	1327	1361	1367	1373
1381	1399	1409	1423	1427	1429	1433	1439	1447	1451
1453	1459	1471	1481	1483	1487	1489	1493	1499	1511
1523	1531	1543	1549	1553	1559	1567	1571	1579	1583
1597	1601	1607	1609	1613	1619	1621	1627	1637	1657
1663	1667	1669	1693	1697	1699	1709	1721	1723	1733
1741	1747	1753	1759	1777	1783	1787	1789	1801	1811
1823	1831	1847	1861	1867	1871	1873	1877	1879	1889
1910	1907	1913	1931	1933	1949	1951	1973	1979	1987
1993	1997	1999	2003	2011	2017	2027	2029	2039	2053

2063	2069	2081	2083	2087	2089	2099	2111	2113	2129
2131	2137	2141	2143	2153	2161	2179	2203	2207	2213
2221	2237	2239	2243	2251	2267	2269	2273	2281	2287
2293	2297	2309	2311	2333	2339	2341	2347	2351	2357
2371	2377	2381	2383	2389	2393	2399	2411	2417	2423
2437	2441	2447	2459	2467	2473	2477	2503	2521	2531
2539	2543	2549	2551	2557	2579	2591	2593	2609	2617
2621	2633	2647	2657	2659	2663	2671	2677	2683	2687
2689	2693	2699	2707	2711	2713	2719	2729	2731	2741
2749	2753	2767	2777	2789	2791	2797	2801	2803	2819
2833	2837	2843	2851	2857	2861	2879	2887	2897	2903
2909	2917	2927	2939	2953	2957	2963	2969	2971	2999
3001	3011	3019	3023	3037	3041	3049	3061	3067	3079
3083	3089	3109	3119	3121	3137	3163	3167	3169	3181
3187	3191	3203	3209	3217	3221	3229	3251	3253	3257
3259	3271	3299	3301	3307	3313	3319	3323	3329	3331
3343	3347	3359	3361	3371	3373	3389	3391	3407	3413
3433	3449	3457	3461	3463	3467	3469	3491	3499	3511
3517	3527	3529	3533	3539	3541	3547	3557	3559	3571
3581	3583	3593	3607	3613	3617	3623	3631	3637	3643
3659	3671	3673	3677	3691	3697	3701	3709	3719	3727
3733	3739	3761	3767	3769	3779	3793	3797	3803	3821
3823	3833	3847	3851	3853	3863	3877	3881	3889	3907
3911	3917	3919	3923	3929	3931	3943	3947	3967	3989
4001	4003	4007	4013	4019	4021	4027	4049	4051	4057
4073	4079	4091	4093	4099	4111	4127	4129	4133	4139
4153	4157	4159	4177	4201	4211	4217	4219	4229	4231
4241	4243	4253	4259	4261	4271	4273	4283	4289	4297
4327	4337	4339	4349	4357	4363	4373	4391	4397	4409
4421	4423	4441	4447	4451	4457	4463	4481	4483	4493
4507	4513	4517	4519	4523	4547	4549	4561	4567	4583
4591	4597	4603	4621	4637	4639	4643	4649	4651	4657
4663	4673	4679	4691	4703	4721	4723	4729	4733	4751
4759	4783	4787	4789	4793	4799	4801	4813	4817	4831
4861	4871	4877	4889	4903	4909	4919	4931	4933	4937
4943	4951	4957	4967	4969	4973	4987	4993	4999	5003
5009	5011	5021	5023	5039	5051	5059	5077	5081	5087

5099	5101	5107	5113	5119	5147	5153	5167	5171	5179
5189	5197	5209	5227	5231	5233	5237	5261	5273	5279
5281	5297	5303	5309	5323	5333	5347	5351	5381	5387
5393	5399	5407	5413	5417	5419	5431	5437	5441	5443
5449	5471	5477	5479	5483	5501	5503	5507	5519	5521
5527	5531	5557	5563	5569	5573	5581	5591	5623	5639
5641	5647	5651	5653	5657	5659	5669	5683	5689	5693
5701	5711	5717	5737	5741	5743	5749	5779	5783	5791
5801	5807	5813	5821	5827	5839	5843	5849	5851	5857
5861	5867	5869	5879	5881	5897	5903	5923	5927	5939
5953	5981	5987	6007	6011	6029	6037	6043	6047	6053
6067	6073	6079	6089	6091	6101	6113	6121	6131	6133
6143	6151	6163	6173	6197	6199	6203	6211	6217	6221
6229	6247	6257	6263	6269	6271	6277	6287	6299	6301
6311	6317	6323	6329	6337	6343	6353	6359	6361	6367
6373	6379	6389	6397	6421	6427	6449	6451	6469	6473
6481	6491	6521	6529	6547	6551	6553	6563	6569	6571
6577	6581	6599	6607	6619	6637	6653	6659	6661	6673
6679	6689	6691	6701	6703	6709	6719	6733	6737	6761
6763	6779	6781	6791	6793	6803	6823	6827	6829	6833
6841	6857	6863	6869	6871	6883	6899	6907	6911	6917
6947	6949	6959	6961	6967	6971	6977	6983	6991	6997
7001	7013	7019	7027	7039	7043	7057	7069	7079	7103
7109	7121	7127	7129	7151	7159	7177	7187	7193	7207
7211	7213	7219	7229	7237	7243	7247	7253	7283	7297
7307	7309	7321	7331	7333	7349	7351	7369	7393	7411
7417	7433	7451	7457	7459	7477	7481	7487	7489	7499
7507	7517	7523	7529	7537	7541	7547	7549	7559	7561
7573	7577	7583	7589	7591	7603	7607	7621	7639	7643
7649	7669	7673	7681	7687	7691	7699	7703	7717	7723
7727	7741	7753	7757	7759	7789	7793	7817	7823	7829
7841	7853	7867	7873	7877	7879	7883	7901	7907	7919
7927	7933	7937	7949	7951	7963	7993	8009	8011	8017
8039	8053	8059	8069	8081	8087	8089	8093	8101	8111
8117	8123	8147	8161	8167	8171	8179	8191	8209	8219
8221	8231	8233	8237	8243	8263	8269	8273	8287	8291
8293	8297	8311	8317	8329	8353	8363	8369	8377	8387

8389	8419	8423	8429	8431	8443	8447	8461	8467	8501
8513	8521	8527	8537	8539	8543	8563	8573	8581	8597
8599	8609	8623	8627	8629	8641	8647	8663	8669	8677
8681	8689	8693	8699	8707	8713	8719	8731	8737	8741
8747	8753	8761	8779	8783	8803	8807	8819	8821	8831
8837	8839	8849	8861	8863	8867	8887	8893	8923	8929
8933	8941	8951	8963	8969	8971	8999	9001	9007	9011
9013	9029	9041	9043	9049	9059	9067	9091	9103	9109
9127	9133	9137	9151	9157	9161	9173	9181	9187	9199
9203	9209	9221	9227	9239	9241	9257	9277	9281	9283
9293	9311	9319	9323	9337	9341	9343	9349	9371	9377
9391	9397	9403	9413	9419	9421	9431	9433	9437	9439
9461	9463	9467	9473	9479	9491	9497	9511	9521	9533
9539	9547	9551	9587	9601	9613	9619	9623	9629	9631
9643	9649	9661	9677	9679	9689	9697	9719	9721	9733
9739	9743	9749	9767	9769	9781	9787	9791	9803	9811
9817	9829	9833	9839	9851	9857	9859	9871	9883	9887
9901	9907	9923	9929	9931	9941	9949	9967	9973	



表 格 目 录



记录的目录



一些最新的记录

2.6 费马数

J.B.Cosgrave 和他的 Proth-Gallot 小组在 2003 年 10 月 10 日发现了一个目前所知道的最大合成费马数. 他们证明了: 746190 位的素数 $3 \cdot 2^{2478785} + 1$ 整除 $F_{2478782}$. 这个记录打破了本小组 8 个月前的结果.

到 2004 年底, 总共知道 217 个费马数为合成数.

2.7 Mersenne 数

采用 GIMPS(见 2.7 节) 发现了两个新的 Mersenne 素数. M. Shafer 于 2003 年 11 月 17 日发现了第 40 个已知的 Mersenne 素数 $2^{20996011} - 1$, 而 J. Findley 于 2004 年 5 月 15 日发现了第 41 个已知的 Mersenne 素数 $2^{24036583} - 1$. 后一个素数有 7235733 位.

指数在 8700000 以下的所有 Mersenne 数现在都检测完毕并做了重复检测.

2.11B 更多的素性检测

素数判定椭圆曲线算法的记录已大为提高. 为了反映这个方法所显示的进步, 让我们比较在一个单处理器的 PC 机 (如 M.Matin 的设备) 上工作的一个程序所实行的检测. 用这种方法所判定出的最大素数为 7760 位的 $E_{2762}/(101 \times 137 \times 193)$. 这里 E_n 为第 n 个欧拉数, 由此得知这个大素数是 E- 不正规的 (定义见作者的著作《关于费马大定理的 13 个讲义》第 203 页). 证明由 M.Oakes

给出，而这个数本身同时也由 D.Broadhurst 所独立决定.

F.Morain 给出素数判定椭圆曲线算法的一个分布式程序，使用个人电脑网络.采用这种设计,证明了 15071 位的奇妙数 $4405^{2638}+2638^{4405}$ 是素数,其素性判定的计算工作是由 J. Franke, T. Kleinjung, F. Morain 和 T. Wirth 完成的.

2.11C 超大素数和奇妙数

到 2004 年 8 月底，目前已知的 5000 个最大素数都超过 50000 位. 目前已知的超过 10^6 的素数有 5 个.

目前所知的最大回文素数是由 H.Dubner 在 2004 年 5 月发现的，它是 120017 位的 $10^{120016}+1726271\times10^{60005}+1$. Dubner 也决定了一些三重回文素数，最大的一个为 98689 位的 $10^{98689}-429151924\times10^{49340}-1$, 是和 J.K.Andersen 一起发现的.

对于由一个数字 d 后面连续一些 9 所构成的素数，新的记录是由 J.Sun 等人于 2004 年 1 月发现的 $9\times10^{107663}-1$ $(d=8)$.

2.11D 因子分解

用特殊的数域筛法 (SNFS) 得到的因子分解记录为将 $2^{1642}+1$ 的因子 $2^{821}+2^{411}+1$ 加以分解，它是 88 位和 160 位的两个素数之积，是由日本人 Aoki,Kida,Shimoyama,Sonoda 和 Ueda 于 2004 年 4 月 4 日宣布的.

用一般的数域筛法所分解的最大数见下面所述.

2.11E 公钥密码体制

新的 RSA 挑战数是按二进制长度方式设计的. 这种挑战数首先被 J.Franke 和 T.Kleinjung 领导的研究小组所分解. 他们于 2003 年 12 月 3 日报告说，成功地分解了 174 位 (对十进制) 的 RSA-576.

用一般数域筛法 (GNFS) 决定出它的两个 87 位的因子.

4.2B 素数间隙

T.Oliviera e Silva 于 2004 年 1 月对于 10^{17} 以内搜索了全部素数间隙值，给出一个新的最大间隙值 $m = 1219$, 其中 $p[m] = 80873624627234849$. 间隙度为 31.31, 是已知的第二大间隙度.

在此之前，只知 $p[1047]$ 的上界，现在知道它就是 $p[1047]$ 的值, 即间隙 $m = 1047$ 第一次发生之处. 于是第一个未确定的 $p[m]$ 值为 $m = 1093$.

目前所知的最大间隙值是 $m = 233821$, 即恰好有连续 233821 个合成数, 由 J.L.Gömez Pardo 所决定. 他还使用 M.Martin ECPP 设备证明了两端 (均为 5878 位数) 是素数，证明于 2003 年 8 月完成.

2004 年 5 月，H.Rosenthal 和 J.K.Andersen 决定了两个 86853 位的数可能为素数，这两个数之间是连续 2254929 个合成数. 如果他们的证明可被严格的验证，这将是第一个被决定的超过 10^6 的素数间隙，间隙度为 11.27.

4.3 孪生素数

以 $\pi_2(x)$ 表示不超过 x 的孪生素数对的个数. P. Sebah 和 P. Demichel 在 2002 年 7 月决定出 $\pi_2(10^{16}) = 10304195697298$. 对于 $h = 1, 2, 3, 4, 5$, 他们算出的 $\pi_2(h \times 10^{15})$ 和 T. Nicely 早先用不同方法独立算出的值完全一致.

在上述计算中，P.Sebah 还给出对 Brun 常数的新估计值 $B = 1.902160583104 \cdots$.

T.Oliveira e Silva 在 2004 年 2 月给出目前所知最大的关于

$\pi_2(x)$ 数值表，由此表知 $\pi_2(10^{17}) = 90948839353159$.

4.4 k- 素数组

只有两种形式的 3- 素数组的记录被打破，由 D.Broadhurst 从 4135 位改进到 4259 位.

4.5C 算术级数中的素数链

M. Frind, P. Jobling 和 P. Underwood 于 2004 年 7 月 24 日发现了算术级数中 23 个素数组成的素数链，第一个素数为 $p = 56211383760397$, 公差为 $d = 44546738095860$. 至此，保持 11 年的记录终于被刷新.

4.6 Goldbach 猜想

T.Oliviera e Silva 对于 2.7×10^{16} 以下的偶数均验证了 Goldbach 猜想.

5.6 数 $k \times b^n \pm 1$

12 个 k 值被认为可能是 Sierpinski 数，其中 $k = 5359$ 在 2003 年 12 月被排除，因为发现了 $5359 \times 2^{5054502} + 1$ 为素数. 这也是目前所知非 Mersenne 素数当中的最大素数. 下表列出这类素数当中最大的 8 个，其中 6 个为广义费马数，而有形式 $3 \times 2^n + 1$ 的两个是目前所知两个最大费马合成数的因子.

形如 $k \times 2^n - 1$ 的已知最大素数为 448724 位的 $2232007 \times 10^{1490605} - 1$, 是 J. Sun, P. Jobling 和 J. Penné 于 2003 年发现的.

形如 $k \times b^n \pm 1$ $(k > 1, b > 2)$ 的最大素数是由 T. Wolter, M. Rodenkirch 等人于 2003 年发现的 $83660 \times 72^{83660} - 1$ (155390 位) 和由 I. Buechel, W. Keller, G. Woltman 和 Y. Gallot 于 2004 年发

现的 $2 \times 4523^{34421} + 1$ (125824 位).

已知的 8 个最大非 Mersenne 素数

素　数	位　数	发　现　者	时间 (年)
$5359 \times 2^{5054502} + 1$	1521561	R.Sundquist, L.Helm, D.Norris et al.	2003
$1372930^{2^{17}} + 1$	804474	D.Heuer, P.Carmody and Y.Gallot	2003
$1361244^{2^{17}} + 1$	803988	D.Heuer, P.Carmody and Y.Gallot	2004
$1176694^{2^{17}} + 1$	795695	D.Heuer, P.Carmody and Y.Gallot	2003
$572186^{2^{17}} + 1$	754652	Y.Gallot, P.Carmody	2004
$3 \times 2^{2478785} + 1$	746190	J.Cosgrave, P.Jobling, G.Woltman and Y.Gallot	2003
$130816^{2^{17}} + 1$	670651	M.Angel, P.Carmody and Y.Gallot	2003
$3 \times 2^{2145353} + 1$	645817	J.Cosgrave, P.Jobling, G.Woltman and Y.Gallot	2003

5.7　素数和二阶线性递归

H.Lifchitz 和 R.Lifchitz 扩大了可能 Fibonacci 素数 U_n 和可能 Lucas 素数 V_n 的清单. 他们加入了 $U_{397379}, U_{433781}, V_{344293}, V_{387433}, V_{443609}, V_{532277}$ 和 V_{574219}, 最后一个数有 120005 位.

数学名著译丛

拓扑空间论

代数特征值问题

数学概观

常微分方程

数学与猜想

代数几何

数学——它的内容，方法和意义

微积分和数学分析引论

代数数理论讲义

非线性及泛函分析——数学分析中的非线性问题讲义

数学的发现——对解题的理解、研究和讲授

代数拓扑基础

博大精深的素数



ISBN 978-7-03-017370-6

定 价：38.00 元